

McDATA[®] 4Gb SAN Switch

for HP p-Class BladeSystem user guide

Legal and notice information

© Copyright 2005 Hewlett-Packard Development Company, L.P.

© Copyright 2005 McDATA Corporation.

© Copyright 2005. This software includes technology under a license from QLogic Corporation. All rights reserved.

Hewlett-Packard Company makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

This document contains proprietary information, which is protected by copyright. No part of this document may be photocopied, reproduced, or translated into another language without the prior written consent of Hewlett-Packard. The information is provided "as is" without warranty of any kind and is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Java is a registered trademark of Sun Microsystems, Inc.

Linux is a registered trademark of Linus Torvalds.

McDATA is a registered trademark of McDATA Corporation.

Microsoft, Windows, Windows 2000/2003, and Windows XP are U.S. registered trademarks of Microsoft Corporation.

Motorola is a registered trademark of Motorola, Inc.

Netscape Navigator and Mozilla are trademarks or registered trademarks of Netscape Communications Corporation.

PowerPC is registered trademark of International Business Machines Corporation.

Red Hat is a registered trademark of Red Hat Software Inc. Adobe[®] and Acrobat[®] are trademarks of Adobe Systems Incorporated.

SANtegrity Enhanced is a trademark of McDATA Corporation.

McDATA Web Server is a trademark of McDATA Corporation.

McDATA[®] 4Gb SAN Switch for HP p-Class BladeSystem user guide

Contents

About this guide	9
Intended audience	9
Prerequisites	9
Related documentation	9
Document conventions and symbols	10
JDOM license	10
HP technical support	11
HP-authorized reseller	11
Helpful web sites	12
1 Using McDATA Web Server	13
Workstation requirements	13
Starting McDATA Web Server	14
Exiting McDATA Web Server	15
Setting McDATA Web Server preferences	15
Using online help	16
Viewing software version and copyright information	16
McDATA Web Server user interface	17
Menu bars	17
Topology display menu	18
Faceplate display menu	18
Shortcut keys	19
Tool bar	19
Fabric tree	20
Graphic window	20
Data window and tabs	20
Working status Indicator	21
Using the topology display	21
Switch and link status	21
Working with switches and links	21
Selecting switches and links	22
Arranging switches in the display	22
Opening the faceplate and topology display popup menus	22
Topology data windows	22
Using the faceplate display	23
Port views and status	23
Working with ports	23
Selecting ports	23
Opening the faceplate popup menu	24
Faceplate data windows	24
2 Managing fabrics	25
RADIUS servers	25
Adding a RADIUS server	26
Removing a RADIUS server	27
Editing RADIUS server information	28
Modifying authentication order RADIUS server information	29
Securing a fabric	30
Connection security	30
User account security	30
Security consistency checklist	30
Device security	31
Edit Security dialog	32
Create Security Set dialog	33

Create Security Group dialog	33
Create Security Group Member dialog	34
Editing the security configuration on a switch	35
Viewing properties of a security set, group, or member	36
Security Config dialog	36
Archiving a security configuration to a file	37
Activating a security set	37
Deactivating a security set	37
Configured Security data window	37
Active Security data window	37
Fabric services	37
Enabling SNMP configuration	38
Enabling in-band management	38
Tracking fabric firmware and software versions	38
Saving a version snapshot	39
Viewing and comparing version snapshots	39
Exporting version snapshots to a file	39
Managing the fabric database	39
Adding a fabric	39
Removing a fabric	40
Opening a fabric view file	40
Rediscovering a fabric	40
Deleting switches and links	40
Adding a new switch to a fabric	41
Replacing a failed switch	41
Displaying fabric information	42
Fabric status	42
Displaying the Event Browser	43
Sorting the Event Browser	45
Filtering the Event Browser	45
Saving the Event Browser to a file	46
Devices data window	46
Active Zone Set data window	47
Link data window	47
Working with device information and nicknames	47
Displaying detailed device information	48
Exporting device information to a file	48
Managing device port nicknames	48
Creating a nickname	49
Editing a nickname	49
Deleting a nickname	49
Exporting nicknames to a file	49
Importing a nicknames file	49
Zoning a fabric	50
Zoning concepts	50
Zones	50
Aliases	50
Zone sets	51
Zoning database	51
Viewing zoning limits and properties	51
Managing the zoning database	52
Editing the zoning database	52
Configuring the zoning database	54
Interop Auto Save	54
Default Visibility	55
Default Zone	55
Discard Inactive	55
Saving the zoning database to a file	55
Restoring the zoning database from a file	55

Restoring the default zoning database	55
Removing all zoning definitions	56
Managing zone sets.	56
Creating a zone set.	56
Activating and deactivating a zone set	57
Copying a zone to a zone set	57
Removing a zone from a zone set or from all zone sets	57
Removing a zone set	57
Managing zones	58
Creating a zone in a zone set	58
Adding zone members	58
Renaming a zone or a zone set	59
Removing a zone member	59
Removing a zone from a zone Set	59
Removing a zone from all zone sets	59
Managing aliases	60
Creating an alias	60
Adding a member to an alias	60
Removing an alias from all zones	60
Merging fabrics and zoning	61
Zone merge failure	61
Zone merge failure recovery.	61
3 Managing switches	63
Managing user accounts	63
Creating user accounts	64
Removing a user account	65
Changing a user account password	66
Modifying a user account	67
Displaying switch information.	68
Devices data window	68
Switch data window	68
Port Statistics data window	71
Port Information data window	71
Configured Zonesets data windows	72
Configuring port threshold alarms.	73
Paging a switch	74
Setting the date/time and enabling NTP client	74
Resetting a switch	75
Configuring a switch.	76
Using the configuration wizard	76
Switch properties	76
Symbolic name.	76
Switch administrative states	77
Domain ID and domain ID lock.	77
Fabric Device Management Interface	78
Broadcast support.	79
In-band management.	79
Advanced switch properties	79
Timeout values	80
Interop mode for zoning	80
System Services dialog.	80
Security Consistency Checklist dialog	81
Network properties	82
IP configuration	82
Remote logging	83
NTP client	83
SNMP properties	83
SNMP configuration	84

SNMP trap configuration	85
Archiving a switch	85
Restoring a switch.	86
Restoring the factory default configuration	87
Downloading a support file	88
Installing Product Feature Enablement (PFE) keys.	88
Installing firmware	89
Using McDATA Web Server to install firmware	89
Using the CLI to install firmware.	90
Displaying hardware status	91
4 Managing ports	93
Displaying port information	93
Monitoring port status	94
Displaying port types	94
Displaying port operational states.	94
Displaying port speeds	95
Displaying transceiver media status.	95
Port Statistics data window	96
Port Information data window	98
Configuring ports	100
Changing port administrative states	100
Changing port speeds	101
Changing port types	101
Device scan	101
Changing port symbolic name.	102
Resetting a port	102
Testing ports	102
5 Command Line Interface.	105
Logging on to a 4Gb SAN Switch	105
User accounts	105
Working with switch configurations	106
Modifying a configuration	106
Backing up and restoring switch configurations	107
Commands	108
Admin command	110
Alias command	111
CIM command	113
CIMListener command.	114
CIMSubscription command	116
Config command	118
Create command	121
Date command.	124
Feature command.	125
Firmware Install command	126
Group command	127
Hardreset command	132
Help command.	133
History command	134
Hotreset command	135
Image command	136
Lip command	139
Passwd command.	140
Ping command	141
Ps command	142
Quit command	143
Reset command	144
Security command	149

Securityset command	152
Set command	154
Set Config command	156
Set Log command	166
Set Port command	169
Set Setup command	170
Show command	178
Show Config command	188
Show Log command	191
Show Perf command	194
Show Setup command	196
Shutdown command	199
Test command	200
Uptime command	202
User command	203
Whoami command	205
Zone command	206
Zoneset command	209
Zoning command	211

Glossary	217
--------------------	-----

Index	221
-----------------	-----

Figures

1 Initial Startup Dialog	14
2 McDATA Web Server window	15
3 Preferences dialog – McDATA Web Server	16
4 McDATA Web Server display elements	17
5 Topology display menu	18
6 Faceplate display menu	18
7 Fabric tree	20
8 Topology display	21
9 Faceplate display	23
10 RADIUS Server Information dialog – Add Server tab page	26
11 RADIUS Server Information dialog – Remove Server tab page	27
12 RADIUS Server Information dialog – Edit Server tab page	28
13 RADIUS Server Information dialog – Modify Authentication Order tab page	29
14 Edit Security dialog	32
15 Create Security Set dialog	33
16 Create Security Group dialog	33
17 Create a Security Group Member dialog	34
18 Security Config dialog	36
19 Fabric Snapshot Analysis dialog	38
20 Add a New Fabric dialog	39
21 Event Browser	44
22 Filter Events dialog	45
23 Active Zone Set data window	47
24 Detailed Device Display dialog	48
25 Edit Zoning dialog	52
26 Zoning Config dialog	54
27 User Account Administration dialog – Add Account tab page	64
28 User Account Administration dialog – Remove Account tab page	65
29 User Account Administration dialog – Change Password tab page	66
30 User Account Administration dialog – Modify Account tab page	67
31 Faceplate display – switch information	68
32 Configured Zonesets data window	72
33 Port Threshold Alarm Configuration dialog	73
34 Port threshold alarm example	74
35 Switch Properties dialog	76

36	Advanced Switch Properties dialog	79
37	System Services dialog	80
38	Network Properties dialog	82
39	SNMP Properties dialog	83
40	Restore dialogs – Full Restore and Selective Restore tab pages	86
41	Features Licenses dialog	89
42	Add License Key dialog	89
43	Hardware status LEDs	91
44	Faceplate display – port information	93
45	Port Properties dialog	100
46	Port Loopback Test dialog	102

Tables

1	Document conventions	10
2	Workstation requirements	13
3	Tool bar buttons	19
4	Topology display switch and status icons	43
5	Severity levels	44
6	Devices data window entries	46
7	Edit Zoning dialog tool bar buttons and icons	53
8	Factory user accounts	63
9	Switch data window entries	69
10	Switch resets	75
11	Switch administrative states	77
12	Corresponding domain ID values by interop mode	78
13	Timeout values	80
14	IP configuration parameters	82
15	SNMP configuration parameters	84
16	SNMP trap configuration parameters	85
17	Factory default configuration settings	87
18	Port types	94
19	Port operational states	94
20	Port speeds	95
21	Port transceiver media view	95
22	Port Statistics data window entries	96
23	Port Information data window entries	98
24	Port administrative states	100
25	Port speeds	101
26	Port types	101

About this guide

This manual describes the McDATA® Web Server™ application switch management tool for the McDATA 4Gb SAN Switch. The McDATA 4Gb SAN Switch is a 10-port non-blocking Fibre Channel (FC) switch. This manual defines the features, components, and performance characteristics of the McDATA 4Gb SAN Switch.

The embedded McDATA Web Server application is the primary focus of this manual which is organized as follows:

- "Using McDATA Web Server" on page 13 describes how to use McDATA Web Server, its menus, and its displays.
- "Managing fabrics" on page 25 describes fabric management tasks.
- "Managing switches" on page 63 describes switch management tasks.
- "Managing ports" on page 93 describes port management tasks.
- "Command Line Interface" on page 105 describes the Command Line Interface (CLI).

A glossary of terms and an index are also provided.

Intended audience

This manual introduces the switch management products and explains their installation and use. It is intended for users responsible for installing and using switch management tools.

Prerequisites

Prerequisites for using this product include:

- Knowledge of operation systems
- Knowledge of related hardware/software

Related documentation

In addition to this guide, please refer to other documents for this product:

- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem release notes AA-RW1ZA-TE*
- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem quick setup instructions A8001-90001*
- *McDATA 4Gb SAN Switch for HP p-Class BladeSystem installation guide AA-RW1XA-TE*

These and other HP documents can be found on the HP documents web site: <http://www.hp.com/support/>.


Document conventions and symbols


Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	<ul style="list-style-type: none">• Key names• Text typed into a GUI element, such as into a box• GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
<i>Italics font</i>	Text emphasis
Monospace font	<ul style="list-style-type: none">• File and directory names• System output• Code• Text typed at the command-line
<i>Monospace, italic font</i>	<ul style="list-style-type: none">• Code variables• Command-line variables
Monospace, bold font	Emphasis of file and directory names, system output, code, and text typed at the command line

 **WARNING!** Indicates that failure to follow directions could result in bodily harm or death.

 **CAUTION:** Indicates that failure to follow directions could result in damage to equipment or data.

 **IMPORTANT:** Provides clarifying information or specific instructions.

 **NOTE:** Provides additional information.

 **TIP:** Provides helpful hints and shortcuts.

JDOM license

This product includes software developed by the JDOM Project (<http://www.jdom.org/>). Copyright (C) 2000—2002 Brett McLaughlin & Jason Hunter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.

3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@jdom.org.
4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management (pm@jdom.org).

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (<http://www.jdom.org/>)."

Alternatively, the acknowledgment may be graphical using the logos available at <http://www.jdom.org/images/logos>.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Brett McLaughlin <brett@jdom.org> and Jason Hunter <jhunter@jdom.org>. For more information on the JDOM Project, please see <<http://www.jdom.org/>>.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: <http://www.hp.com/support/>.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

For continuous quality improvement, calls may be recorded or monitored.

HP strongly recommends that customers sign up online using the Subscriber's choice web site: <http://www.hp.com/go/e-updates>.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP-authorized reseller

For the name of your nearest HP-authorized reseller:

- In the United States, call 1-800-282-6672.
- Elsewhere, visit the HP web site: <http://www.hp.com>. Then click **Contact HP** to find locations and telephone numbers.

Helpful web sites

For other product information, see the following HP web sites:

- <http://www.hp.com>
- <http://www.hp.com/go/storage>
- <http://www.hp.com/support/>
- <http://www.docs.hp.com>
- <http://h71028.www7.hp.com/enterprise/cache/80316-0-0-0-121.html>

1 Using McDATA Web Server

This section describes how to use the McDATA Web Server application and its menus. The following topics are covered:

- [Workstation requirements](#), page 13
- [Starting McDATA Web Server](#), page 14
- [Exiting McDATA Web Server](#), page 15
- [Setting McDATA Web Server preferences](#), page 15
- [Using online help](#), page 16
- [Viewing software version and copyright information](#), page 16
- [McDATA Web Server user interface](#), page 17
- [Using the topology display](#), page 21
- [Using the faceplate display](#), page 23

Workstation requirements

The requirements for fabric management workstations running McDATA Web Server are described in [Table 2](#).

Table 2 Workstation requirements

Operating System	Windows® 2000, 2003 Linux® Red Hat® EL 3.x, 4.x
Memory	256 MB or more
Disk Space	150 MB per installation
Processor	500 MHz or faster
Hardware	RJ-45 Ethernet port
Internet Browser	Microsoft® Internet Explorer® 5.0 or later Netscape® Navigator® 4.72 or later Mozilla™ 1.02 or later Java 2 Run Time Environment installed to support the Web Server. Refer to Starting McDATA Web Server , page 14 for more information.

Starting McDATA Web Server

To start McDATA Web Server after the switch is operational, enter the switch IP address in an internet browser. The workstation used to manage the switch must be able to connect to the default switch IP address 10.0.0.1.

1. At the workstation, enter the default switch IP address (10.0.0.1) in an internet browser. If your workstation does not have the Java 2 Run Time Environment program, you will be prompted to download it.
2. Click **Proceed** in the Initial Start Dialog of the McDATA Web Server window.
3. Enter the default switch IP address, login name (default is “admin”), and password (default is “password”) in the Add a New Fabric window.
4. Click **Add Fabric**.
5. Select the switch in the graphic window of the topology display.
6. Select **Switch > Network Properties**.
7. Change the **IP Address**, **Subnet Mask**, and **Gateway** settings to reflect your desired network configuration in the Network Properties dialog.
8. Click **OK**.
9. Select **File > Exit** to close the McDATA Web Server application. The switch is now ready to be managed through your network.
10. Repeat steps 1—4 using the switch's newly configured IP address to launch the McDATA Web Server application once your configured switch is connected to the network.

The application opens with the Initial Start Dialog shown in [Figure 1](#). Select **Don't show this dialog again** if you prefer not to see this dialog again. This has the same effect as disabling the Display Initial Startup Dialog preference. Refer to “[Setting McDATA Web Server preferences](#)” on page 15 for information about setting preferences.



Figure 1 Initial Startup Dialog

Perform one of the following procedures to access and begin managing the switch:

- Select **Open Existing Fabric** to open the Add a New Fabric dialog, which prompts you for a fabric name, IP address, account name, and password. Refer to “[Adding a fabric](#)” on page 39.

- Select **Start Application Without Specifying a Fabric** to open the McDATA Web Server window shown in [Figure 2](#). Click **Add** to open the Add a New Fabric dialog, which prompts you for a fabric name, IP address, account name, and password. Refer to ["Adding a fabric"](#) on page 39.

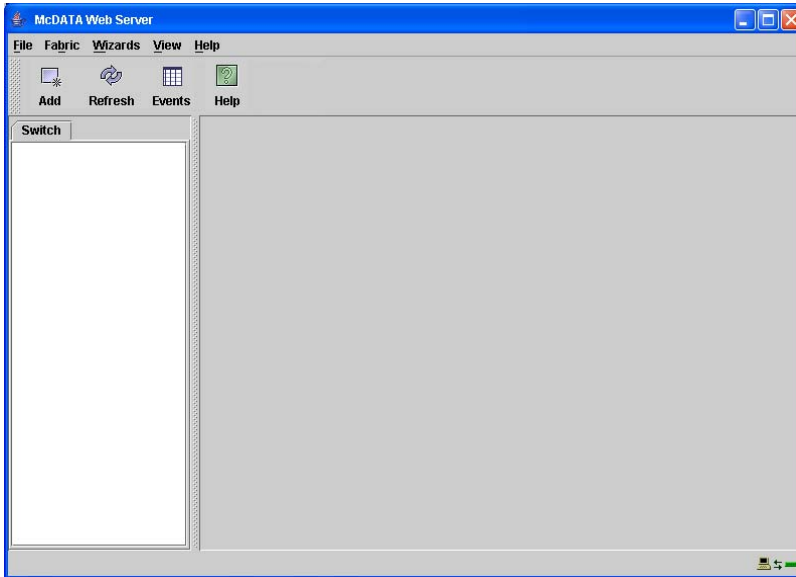


Figure 2 McDATA Web Server window

Exiting McDATA Web Server

Select **File > Exit** to exit a McDATA Web Server application session. Enter the password and click **OK**, if the fabric view file was saved with a password.

Setting McDATA Web Server preferences

Using the preferences settings, you can:

- Change the location of the working directory in which to save files.
- Change the location of the browser used to view the online help.
- Enable (default) or disable the use of the Initial Start Dialog at the beginning of a McDATA Web Server session. Refer to ["Starting McDATA Web Server"](#) on page 14 for information about the Initial Start Dialog. After a default fabric view file is created, this setting has no effect.
- Enable (default) or disable the Event Browser. Refer to ["Displaying the Event Browser"](#) on page 43. If the Event Browser is enabled using the Preferences dialog as shown in [Figure 3](#), the next time McDATA Web Server is started, all events will be displayed. If the Event Browser is disabled when McDATA Web Server is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.
- Choose the default port view when opening the faceplate display. You can set the faceplate to reflect the current port type (default), port speed, port operational state, or port transceiver media. Regardless of the default port view you choose, you can change the port view in the faceplate display by opening the View menu and selecting a different port view option. Refer to the corresponding subsection for more information:
 - [Displaying port types](#), page 94
 - [Displaying port operational states](#), page 94
 - [Displaying port speeds](#), page 95

- [Displaying transceiver media status](#), page 95

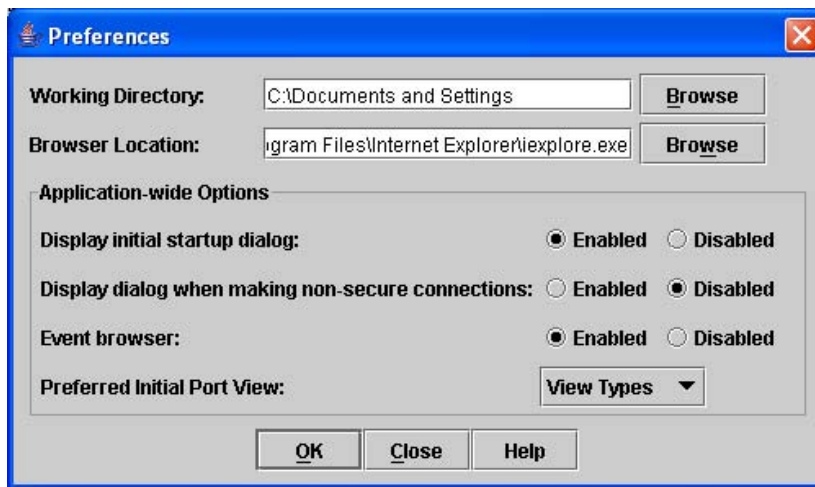


Figure 3 Preferences dialog – McDATA Web Server

To set preferences for your McDATA Web Server sessions, perform the following procedure:

1. Select **File > Preferences** to open the Preferences dialog.
2. Enter or browse for paths to the working directory and browser.
3. Choose the preferences you want in the Application-wide Options area.
4. Click **OK** to save the changes.

Using online help

Online help is available for the McDATA Web Server application and its functions. To open online help, choose one of the following:

- Select **Help > Help Topics**.
- Click **Help** in the tool bar.
- Click **Help** in McDATA Web Server dialogs to display context-sensitive help in dialogs.

Viewing software version and copyright information

Select **Help > View** to view McDATA Web Server software version and copyright information.

McDATA Web Server user interface

The McDATA Web Server application uses two basic displays to manage the fabric and individual switches: the topology display and the faceplate display. The topology display shows all switches that are able to communicate and all connections between switches. The faceplate display shows the front of a single switch and its ports. Both displays share some common elements as shown in Figure 4.

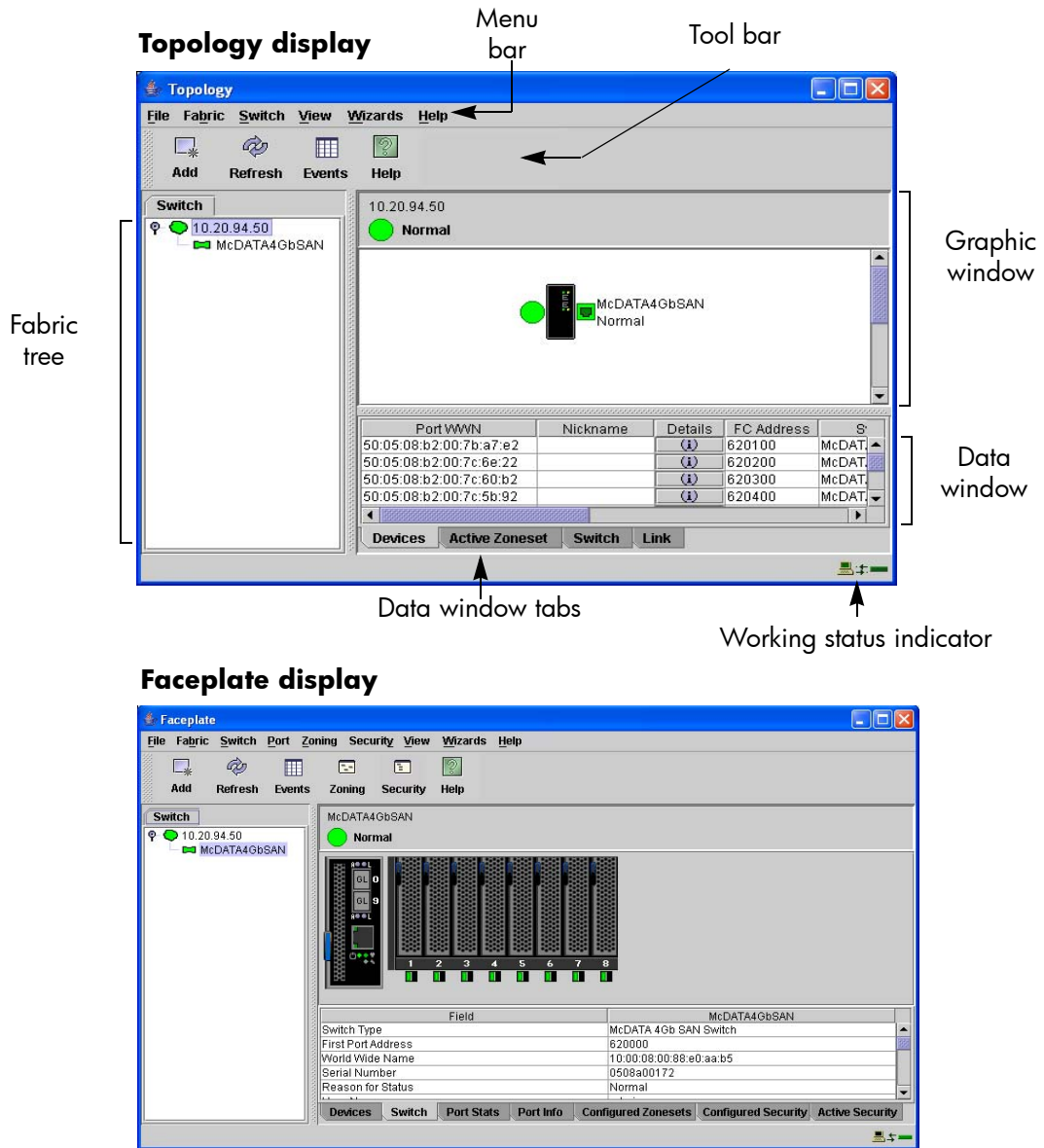


Figure 4 McDATA Web Server display elements

Menu bars

The menus and the options offered in them vary depending on the display. For example, the Port menu and many of the Switch menu selections are available only in the faceplate display.

Topology display menu

The menu options available in the topology display are shown in [Figure 5](#).

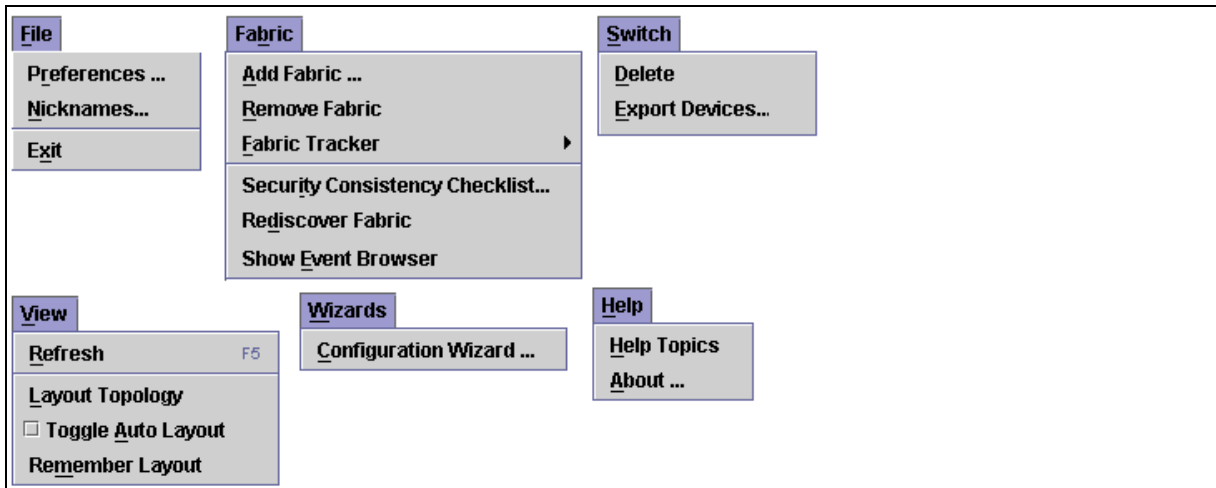


Figure 5 Topology display menu

Faceplate display menu

The menu options available in the faceplate display are shown in [Figure 6](#).

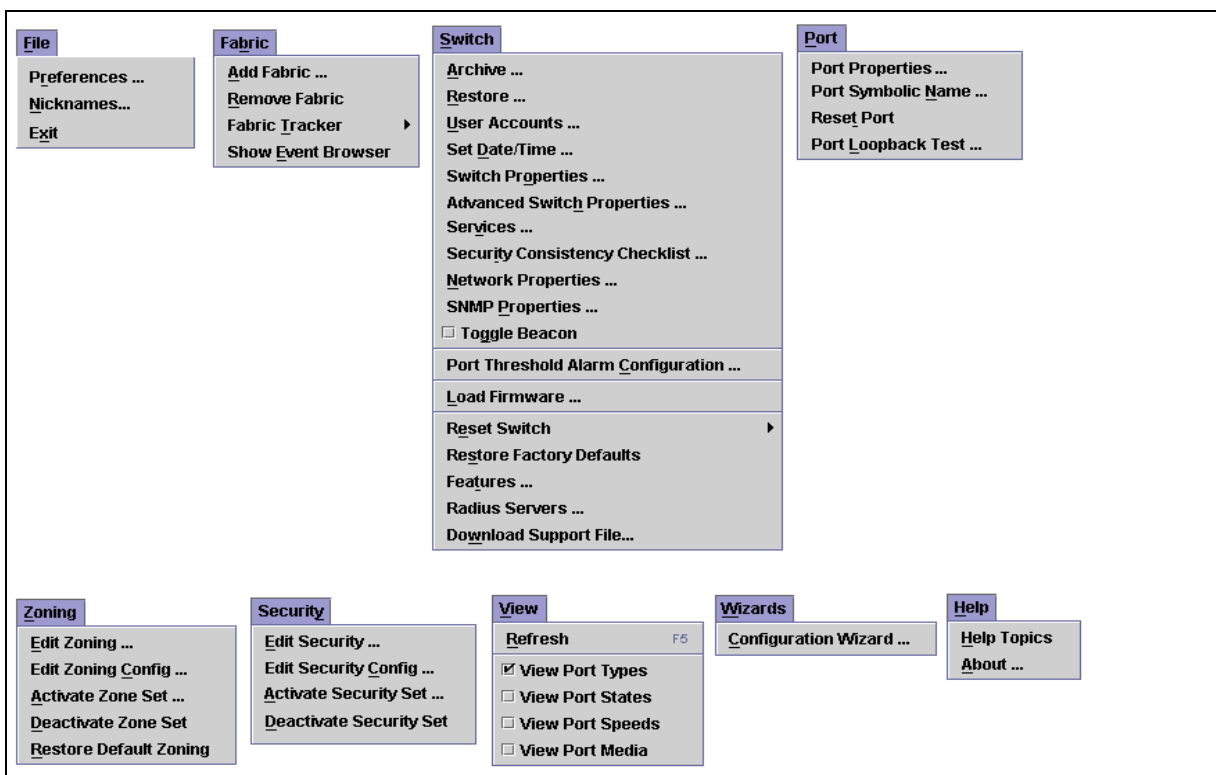


Figure 6 Faceplate display menu

 **NOTE:** The Security menu is only displayed if Secure Sockets Layer (SSL) is enabled. Select **Switch > Services > SSL** to enable SSL. Refer to “[System Services dialog](#)” on page 80 for more information.

The keyboard shortcut keys vary by display type: topology display and faceplate display. In addition to the menu bar, both the topology and faceplate displays have context-sensitive menus that pop up when you right-click in the graphic window. Refer to “[Opening the faceplate and topology display popup menus](#)” on page 22 for more information about these popup menus.







Shortcut keys

Shortcut key combinations, available in both the topology and faceplate displays, provide an alternative method of accessing menu options. The shortcut key combinations are not case-sensitive. For example, to exit the application, press **Alt+F > X**.

Tool bar

The tool bar consists of a row of graphical buttons that you can use to access McDATA Web Server functions as shown in [Table 3](#). The tool bar buttons are an alternative method to using the menu bar. The tool bar can be relocated in the display by clicking and dragging the handle at the left edge of the tool bar.

Table 3 Tool bar buttons

Tool bar button	Description
 Add	Add Fabric button — adds a new fabric to the fabric view
 Refresh	Refresh button — updates the topology or faceplate display with current information
 Events	Event Browser button — opens the events browser
 Zoning	Edit Zoning button — opens the Edit Zoning dialog (available only in faceplate display)
 Security	Edit Security button — opens the Edit Security dialog (faceplate display only)
 Help	Help Topics button — opens the online help file

Fabric tree

The fabric tree lists the managed fabrics and their switches as shown in [Figure 7](#). The window width can be adjusted by clicking and dragging the moveable window border. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded or collapsed. Click this handle or double-click the entry to expand or collapse a fabric tree entry. A fabric entry expands to show its member switches.

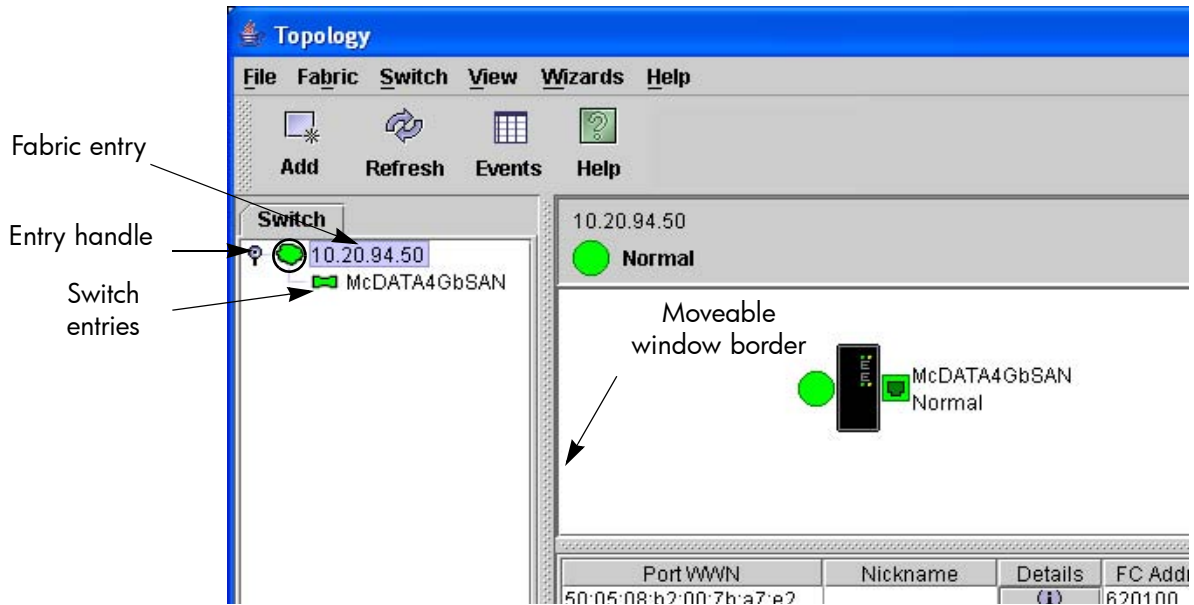


Figure 7 Fabric tree

Each fabric tree entry has a small icon next to it that uses color to indicate operational status.

- A green icon indicates normal operation.
- A yellow icon indicates that a switch is operational, but may require attention to maintain maximum performance.
- A red icon indicates a potential failure or non-operational state as when the switch is offline.
- A blue icon indicates that a switch is unknown, unreachable, or unmanageable.
 - If the status of the fabric is not normal, the fabric icon in the fabric tree will indicate the reason for the abnormal status. The same message is provided when you rest the mouse over the fabric icon in the fabric tree.
 - The fabric tree provides access to the topology and faceplate displays for any fabric or switch.
- Click a fabric entry in the fabric tree to open the topology display.
- Click a switch entry in the fabric tree to open the faceplate display.

Graphic window

The graphic window, shown in [Figure 4](#), presents graphic information about fabrics and switches such as the fabric topology and the switch faceplate. The window height can be adjusted by clicking and dragging the window border that it shares with the data window.

Data window and tabs

The data window presents a table of data and statistics associated with the selected tab. Use the scroll bar to browse through the data. The window length can be adjusted by clicking and dragging the border that it shares with the graphic window.

Adjust the column width by moving the pointer over the column heading border shared by two columns until a right/left arrow graphic is displayed. Click and drag the arrow to the desired width.

The data window tabs present options for the type of information to display in the data window. These options vary depending on the display.

Working status Indicator

The working status indicator, located in the lower right corner of the McDATA Web Server window, shows when the management workstation is exchanging information with the fabric. As conditions change, the fabric forwards this information to the management workstation where it is reflected in the various displays.

Using the topology display

The topology display shown in [Figure 8](#) receives information from the selected fabric and displays its topology. Switches and inter-switch links (ISLs) appear in the graphic window and use color to indicate status. Consider the following topology display features:

- [Switch and link status](#), page 21
- [Working with switches and links](#), page 21
- [Topology data windows](#), page 22

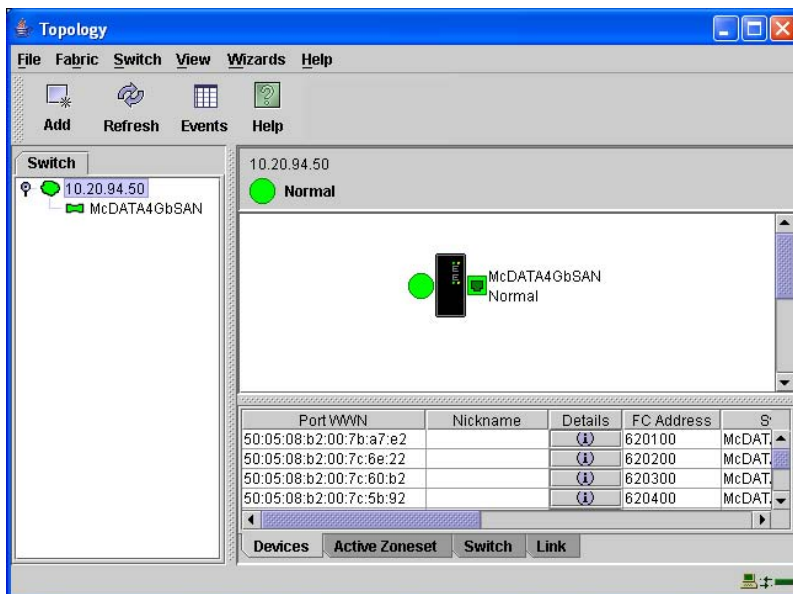


Figure 8 Topology display

Switch and link status

Switch icon shape and color provide information about the switch and its operational state. Lines represent links between switches. The topology display uses green to indicate normal operation, yellow to indicate operational with errors, red to indicate a potential failure or non-operational state, and blue to indicate unknown, unreachable, or unmanageable. Refer to "[Fabric status](#)" on page 42 for more information about topology display icons.

Working with switches and links

Switch and link icons are selectable and moveable, and serve as access points for other displays and menus. You select switches and links to display information about them, modify their configuration, or delete them from the display. Context-sensitive popup menus are displayed when you right-click on a switch or link icon, or in the background of the topology display graphic window.

Selecting switches and links

Selected switch icons are highlighted in light blue. Selected ISLs are displayed as a heavier line. You can select switches and links in the following ways:

- Click the icon or link to select a switch or a link.
- Press and hold **Control**, and select multiple switches or links.
- Right-click anywhere in the graphic window background to select all switches or links. Select **Select > All Switches**, or select **Select > Select All Links** from the popup menu.
- Press and hold **Control**, and select the item again to cancel a selection. Click in the graphic window background to cancel all selections.

Arranging switches in the display

You can arrange individual switch icons in the topology display or allow McDATA Web Server to arrange all switch icons for you:

- Click and drag the icon to another location in the graphic window to move an individual switch icon. Links stretch or contract to remain connected.
- Select **View > Layout Topology** to arrange all switch icons in the topology display automatically.

By default, the Toggle Auto Layout box in the View menu is checked which causes McDATA Web Server to arrange the icons when you select **Layout Topology**.

You can save a custom arrangement, or layout, and restore that layout during a McDATA Web Server session. Begin by arranging the icons, then select **View > Remember Layout**. Un-select **Toggle Auto Layout > Layout Topology** to restore the saved layout.

Opening the faceplate and topology display popup menus

The topology display shows all switches that are able to communicate and all connections between switches. The faceplate display shows the front of a single switch and its ports. Menu options vary with each type of popup menu.

- Right-click the graphic window background to open the fabric popup menu in the topology display.
- Right-click the switch icon in the graphic window to open the switch popup menu in the topology display.
- Right-click the link to open the link popup menu in the topology display.
- Right-click the faceplate in the graphic window to open the switch popup menu in the faceplate display.

Topology data windows

The topology display provides the following data windows corresponding to the data window tabs:

- Devices – displays information about devices (hosts and storage targets) connected to the switch. Refer to “[Devices data window](#)” on page 68 for more information.
- Active Zoneset – displays the active zone set for the fabric including zones and their member ports. Refer to “[Active Zone Set data window](#)” on page 47 for more information about this data window. Refer to “[Zoning a fabric](#)” on page 50 for information about zone sets and zones.
- Switch – displays current network and switch configuration data for the selected switches. Refer to “[Switch data window](#)” on page 68 for more information.
- Link – displays information about the inter-switch links. Refer to “[Link data window](#)” on page 47 to for more information.

Using the faceplate display

The faceplate display shown in [Figure 9](#) displays the switch name and operational state, and port status. The external ports numbered 0 and 9. Internal ports are numbered 1–8. The port numbers 1–8 correspond to server blades slots 1–8.

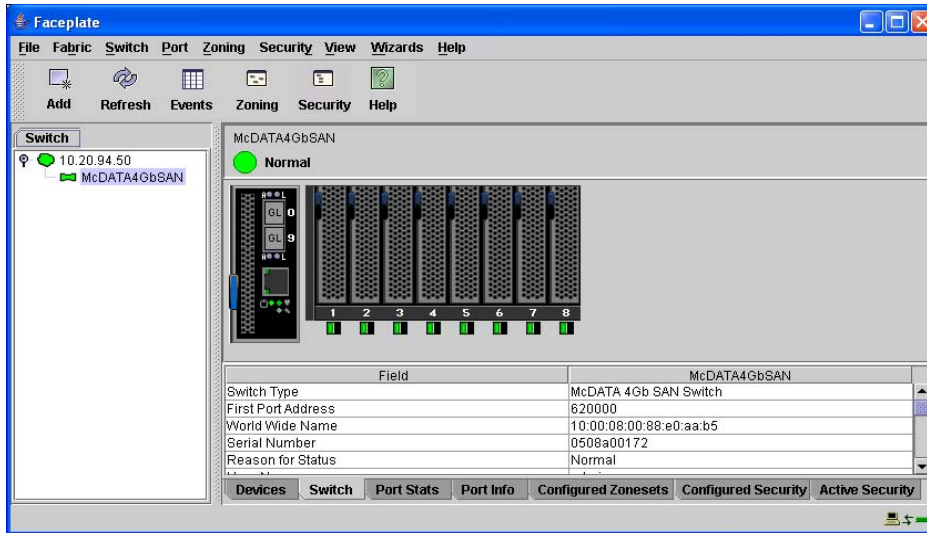


Figure 9 Faceplate display

Consider the following functional elements of the faceplate display:

- [Port views and status](#), page 23
- [Working with ports](#), page 23
- [Faceplate data windows](#), page 24

Port views and status

Port color and text provide information about the port and its operational state. Green indicates active; gray indicates inactive. The faceplate display provides the following views of port status corresponding to the View menu options in the faceplate display. Refer to [“Monitoring port status”](#) on page 94 for more information about these displays.

- Port type
- Port state
- Port speed
- Port media

Right-click the faceplate image or a port icon in the faceplate to display context-sensitive popup menus.

Working with ports

Ports are selectable and serve as access points for other displays and menus. You select ports to display information about them in the data window or to modify them. Right-click the faceplate image or on a port icon in the faceplate to display context-sensitive popup menus.

Selecting ports

You can select ports in the following ways. Selected ports are outlined in white.

- Click the port in the faceplate display to select a port.
- Select a port, then press and hold **Shift**, and select another port to select a range of consecutive ports. The application selects both end ports and all ports in between in port number sequence.
- Press and hold **Control** while selecting ports to select several non-consecutive ports.
- Press and hold **Control**, and click a selected port to cancel that selection.

Opening the faceplate popup menu

To open the popup menu, right-click on the faceplate image to present the following tasks.

- Refresh the switch
- Select all ports
- Manage switch properties
- Manage network properties
- Manage SNMP properties
- Manage port properties
- Change the port symbolic name
- Run the port loopback tests
- Services
- Security Consistency Checklist

If no ports are selected, the port-related tasks will be unavailable in the menu. Right-click a port to open the Port popup menu. Press and hold **Shift** or **Control** to select more than one port. Right-click one of the selected ports to unselect multiple ports.

Faceplate data windows

The faceplate display provides the following data windows corresponding to the data window tabs:

- Devices — displays information about devices (hosts and storage targets) connected to the switch.
- Switch — displays current switch configuration data.
- Port Statistics — displays performance data for the selected ports.
- Port Information — displays information for the selected ports.
- Configured Zonesets — displays all zone sets, zones, and zone membership in the zoning database.
- Configured Security — displays all security definitions currently saved in the database.
- Active Security — displays the active security set.

2 Managing fabrics

This section describes the following tasks that manage fabrics:

- [RADIUS servers](#), page 25
- [Securing a fabric](#), page 30
- [Tracking fabric firmware and software versions](#), page 38
- [Managing the fabric database](#), page 39
- [Displaying fabric information](#), page 42
- [Working with device information and nicknames](#), page 47
- [Zoning a fabric](#), page 50

RADIUS servers

Remote Authentication Dial In User Service (RADIUS) provides a method to centralize the management of authentication passwords in larger networks. It has a client/server model, where the server is the password repository and third party authentication point and the clients are all of the managed devices. RADIUS can be configured for devices and/or user accounts. The RADIUS server dialogs are available only on a secure (SSL) fabric and on the entry switch (out of band switch). Refer to "[Connection security](#)" on page 30 and "[System Services dialog](#)" on page 80 for more information.

RADIUS is designed to authenticate users and devices using a challenge/response protocol. Basic implementations consist of a central RADIUS server containing a database of authorized users as well as authentication information. A RADIUS client wishing to verify the authenticity of a user issues a challenge to the user and collects the response to the challenge. This information is forwarded to the RADIUS server for authentication and the server responds with the results, either an accept or reject. The RADIUS client does not need to be configured with any user authentication information, this all resides on the RADIUS server and can be managed centrally and separately from the clients. In addition, no passwords are exchanged between the RADIUS server and its clients. Authentication of requests from a RADIUS client to the server and responses from the server to a client can also be authenticated. This requires sharing a secret between the server and client. The accounting RADIUS supports the auditing of the users and switch services such as Telnet, FTP, and switch management applications. The RADIUS Accounting Server enables (True) or disables (False) the auditing of activity during a user session. The default is False. When enabled, user activity is audited whether UserAuthServer is enabled or not. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).

Adding a RADIUS server

When you add a RADIUS server, you provide a method to centralize the management of authentication passwords over a network.

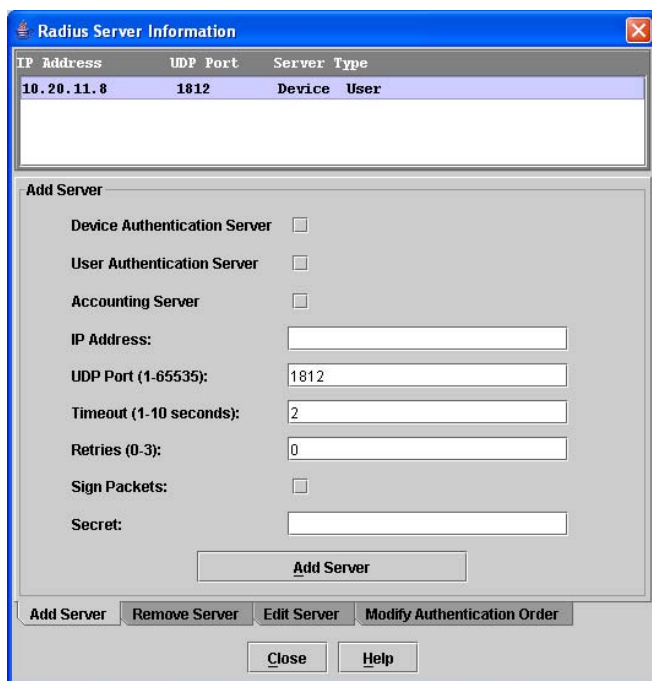


Figure 10 RADIUS Server Information dialog — Add Server tab page

To add a RADIUS server, perform the following procedure:

1. Select **Switch > RADIUS Servers** in the faceplate display.
2. Click the **Add Server** tab in the Radius Server Information dialog shown in [Figure 10](#).
3. Select **Device**, **User**, or **Account** for the server type.
4. Enter the remote IP address of the server in the **IP Address** field.
5. Enter the remote UDP port number of the Authentication RADIUS Server in the **UDP Port** field.
The RADIUS Accounting Server UDP port will always be the value of Device/User Authentication Server UDP Port + 1. When enabled, the RADIUS Accounting Server audits user activity whether UserAuthServer is enabled or not. The RADIUS Accounting Server default is False.
6. Enter the timeout value in seconds (minimum of 1 second, maximum of 30 seconds) in the **Timeout** field. This is the number of seconds the RADIUS client will wait for a response from the RADIUS server before retrying, or giving up on a request.
7. Enter the number of retries in the **Retries** field. This is the maximum number of times the RADIUS client will retry a request sent to the primary RADIUS server.
8. Select **Sign Packet** to enable the switch to include a digital signature (Message-Authenticator) in all RADIUS access request packets sent to the RADIUS server. A valid Message-Authenticator attribute will be required in all RADIUS server responses.
9. Enter the server secret in the **Secret** field. A secret is required for all RADIUS servers. The secret is used when generating and checking the Message-Authenticator attribute.
10. Click **Add Server** to add the server.
11. Click **Modify Authentication Order** tab, and verify that **Device Authentication Order** and **User Authentication Order** options are set to either **Radius** or **Radius Local** for RADIUS Authentication to be implemented. Refer to "[Modifying authentication order RADIUS server information](#)" on page 29 for more information.
 - a. **RADIUS** — only attempts to authenticate using the RADIUS server (another computer that provides authentication).

- b. **RADIUS Local** — attempts to authenticate using the RADIUS server. If the switch can not contact the RADIUS server due to a network or some other problem, the switch will authenticate using the local password database.

12. Click **Close** to close the Radius Server Information dialog.

Removing a RADIUS server

When you remove a RADIUS server, you disable the management of authentication usernames and passwords over the network for that server.

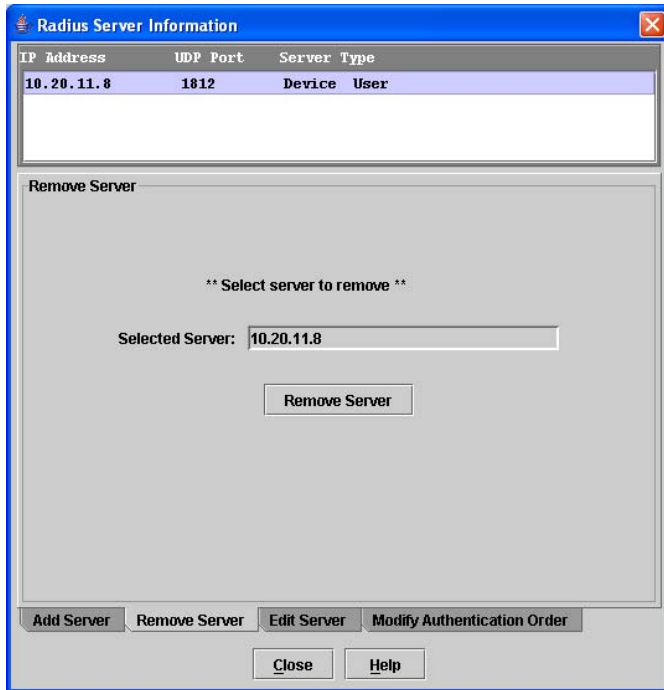


Figure 11 RADIUS Server Information dialog — Remove Server tab page

To remove a RADIUS server, perform the following procedure:

1. Select **Switch > RADIUS Servers** in the faceplate display.
2. Click the **Remove Server** tab in the Radius Server Information dialog shown in [Figure 11](#).
3. Select the server to be removed in server list at the top of the dialog.
4. Click **Remove Server** to remove the server.
5. Click **Close** to close the Radius Server Information dialog.

Editing RADIUS server information

Editing information of a RADIUS server involves changing the configuration of a RADIUS server.

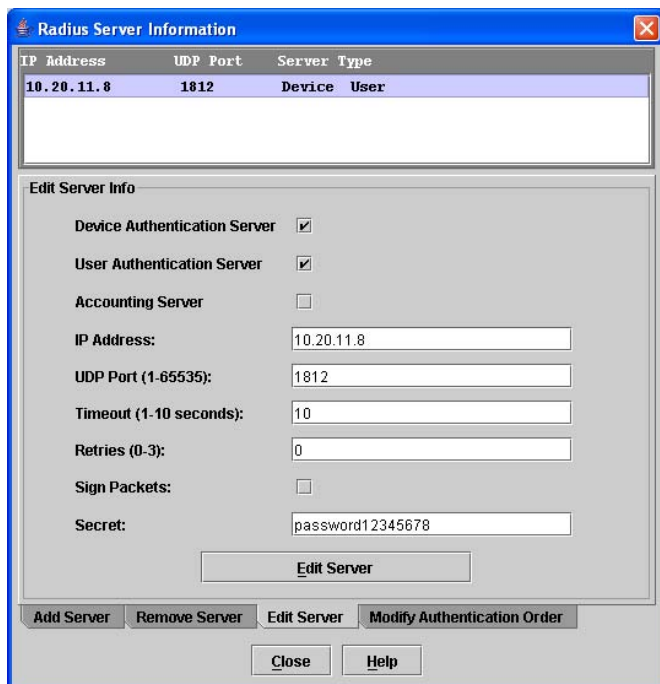


Figure 12 RADIUS Server Information dialog — Edit Server tab page

To edit information of a RADIUS server, perform the following procedure:

1. Select **Switch > Radius Servers** in the faceplate display.
2. Click the **Edit Server** tab in the Radius Server Information dialog shown in [Figure 12](#).
3. Select the server to be edited in server list at the top of the dialog.
4. Make changes to the **IP Address**, **UDP Port**, **Timeout**, **Retries**, and **Secret** fields.
5. Select the server type (**Device**, **User**, **Account**) and **Sign Packet** options.
6. Click **Edit Server** to save the changes.
7. Click **Close** to close the Radius Server Information dialog.

Modifying authentication order RADIUS server information

Editing information of a RADIUS server involves changing the configuration of a RADIUS server.

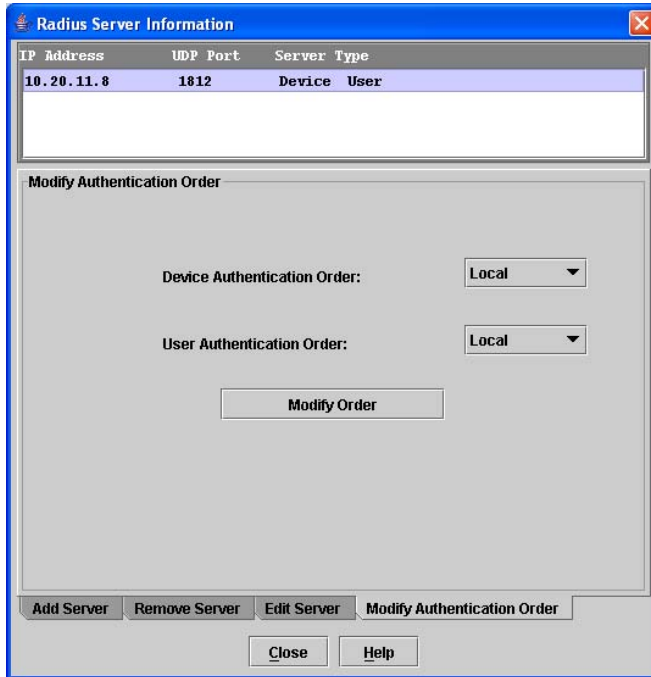


Figure 13 RADIUS Server Information dialog — Modify Authentication Order tab page

To modify the authentication order information of a RADIUS server, perform the following procedure:

1. Select **Switch > Radius Servers** in the faceplate display.
2. Click the **Modify Authentication Order** tab in the Radius Server Information dialog shown in [Figure 13](#).
3. Select the server to be modified in server list at the top of the dialog.
4. Make changes to the **Device Authentication Order** or **User Authentication Order** drop-down lists. Select one of the following:
 - a. **Local** — only attempts to authenticate using local switch password database.
 - b. **RADIUS** — only attempts to authenticate using the RADIUS server (another computer that provides authentication).
 - c. **RADIUS Local** — attempts to authenticate using the RADIUS server. If the switch can not contact the RADIUS server due to a network or some other problem, the switch will authenticate using the local password database.
5. Click **Modify Order** to save the changes.
6. Click **Close** to close the Radius Server Information dialog.

Securing a fabric

Fabric security consists of the following:

- [Connection security](#), page 30
- [User account security](#), page 30
- [Security consistency checklist](#), page 30
- [Device security](#), page 31
- [Fabric services](#), page 37

Connection security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the CLI and the Secure Socket Layer (SSL) protocol for management applications such as McDATA Web Server and Common Information Module (CIM).


The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. The switch certificate is valid for one year beginning with its creation date and time. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. If a certificate has not been created by the user, the switch will automatically create one.

Consider your requirements for connection security: for the CLI (SSH), management applications such as McDATA Web Server (SSL), or both. If SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize date/time between workstations and switches.

User account security


User account security is the process by which your user account and password are authenticated with the list of valid user accounts and passwords. The switch validates your account and password when you attempt to add a fabric using McDATA Web Server or log in to a switch through Telnet. Your system administrator defines accounts, passwords, and authority levels that are stored on the switch. Refer to "[Managing user accounts](#)" on page 63 for more information.

The Admin account possesses Admin authority which grants full access to all tasks of the McDATA Web Server menu system. The switch validates your user account and McDATA Web Server grants access to its menus according to your authority level. If you do not have Admin authority, you are limited to monitoring tasks.

 **NOTE:** If a user is logged into a switch using McDATA Web Server or CLI, and an administrator changes user access rights and passwords, existing login sessions will not be affected by the new settings. Login access and privileges are only checked for a new login request.

Security consistency checklist

The Security Consistency Checklist dialog enables you to compare security-related features on switches to check for inconsistencies. Any changes must be made through the appropriate dialog, such as Network Properties dialog, Switch Properties dialog, or SNMP Properties dialog. Select **Switch > Security Consistency Checklist** to open the Security Consistency Checklist dialog.

 **IMPORTANT:** Device security is available only with the McDATA SANtegrity™ Product Feature Enablement (PFE) key. Refer to “Installing Product Feature Enablement (PFE) keys” on page 88 for more information about installing a PFE key. To obtain the McDATA 4Gb SAN Switch serial number and Product Feature Enablement key, follow the step-by-step instructions on the “firmware feature entitlement request certificate” for the PFE key. One of the license key retrieval options is via the web: www.webkey.external.hp.com.

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch security database, or remotely using a Remote Dial-In User Service (RADIUS) server. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to be distributed on the switches or centralized on a RADIUS server and how many servers to configure.

Managing device security involves the following tasks:

- Creating security sets, groups, and members
- Editing a security configuration on a switch
- Viewing properties of a security set, group, or member
- Archiving a security configuration on a switch to a file
- Activating and deactivating a security set

The security database is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of security groups is 16.
- Maximum number of members in a group is 1000.
- Maximum total number of group members is 1000.

Edit Security dialog

Use the Edit Security dialog to edit the security configuration on the switch. You can also open and edit a security configuration saved to a file. Editing security files consists of renaming and removing security sets, groups, and members. The Security dialogs are available only on a secure (SSL) fabric and on the entry switch (out of band switch).

To open the Edit Security dialog shown in [Figure 14](#), choose one of the following:

- Click **Security** in the tool bar.
- Select **Security > Edit Security**.

 **NOTE:** The Security menu and button are only displayed if Secure Sockets Layer (SSL) is enabled. Select **Switch > Services > SSL** to enable SSL. Refer to "[System Services dialog](#)" on page 80 for more information.

Use the Edit menu options or popup menu options to access Edit Security dialog options. Select a security item in the graphic window and select an option in the Edit menu, or right-click on a security item in the graphic window, and select an option from the popup menus.

The orphan security set contains the security groups and members that don't belong to a user-defined security set. Excluding the orphan security set, you can only have 1 group type in a security set. The three types of security groups are:

- ISL — default (E_Port authentication)
- MS (Management Server CT authentication)
- Port (F_Port authentication)



Figure 14 Edit Security dialog

Use the File menu in the Edit Security dialog to:

- Edit the security configuration on the switch.
- Open or edit security files.
- Save or rename security files

Use the Edit menu in the Edit Security dialog to:

- Create security sets, security groups, and security group members.
- Rename or remove a security group from a security set or a member from a security group.
- Remove a group from all security sets.
- Remove all security sets, groups, or members.

- View properties for the selected security set, group, or group member.

Create Security Set dialog

Use the Create Security Set dialog shown in [Figure 15](#) to create a new security set. There is a maximum of 4 security sets.

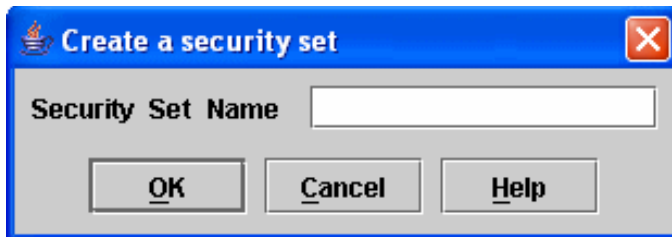


Figure 15 Create Security Set dialog

To add a security set from the faceplate display, perform the following procedure:

1. Click **Security** on the tool bar, or select **Security > Edit Security** to open the Edit Security dialog.
2. To open the Create a Security Set dialog, choose one of the following:
 - Click **Security Set** in the Edit Security dialog tool bar.
 - Right-click in the graphic window of the Edit Security dialog, and select **New Security Set** from the popup menu.
3. Enter a name for the new security set. The naming conventions for security sets are:
 - Must start with a letter.
 - All alphanumeric chars [aA—zZ] [0—9].
 - The symbols \$ _ - and ^ are the only symbols allowed.
4. Click **OK** to save the change.

Create Security Group dialog

Use the Create Security Group dialog, shown in [Figure 16](#), to add a security group to a security set. To open the Create a Security Group dialog, choose one of the following:

- Click **Security Group** in the Edit Security dialog tool bar.
- Right-click in the graphic window of the Edit Security dialog, and select **Create a Security Group** from the popup menu.



Figure 16 Create Security Group dialog

The naming conventions for all security groups are listed below.

- Must start with a letter.
- All alphanumeric chars [aA—zZ] [0—9].
- The symbols \$ _ - and ^ are the only symbols allowed.

An empty (no members) security group in the active security set will prevent all connections for that security group type. For example, an empty ISL security group will cause the switch to refuse all logins from other switches. To add a security group to a security set, perform the following procedure:

1. Click **Security** on the tool bar in the faceplate display or select **Security > Edit Security** to open the Edit Security dialog.

2. Choose one of the following methods to open the Create a Security Group dialog:
 - Click a security set and click **Security Group** in the tool bar in the graphic window.
 - Right-click on a security set and select **Create a Security Group** from the popup menu.
3. Enter a security group name and select a security group type (ISL, Port, or MS). Remember, only one security group type (1 ISL, 1 Port, 1 MS) in each security set is allowed. The naming conventions for security groups are:
 - Must start with a letter
 - All alphanumeric chars [aA–zZ] [0–9]
 - The symbols \$ _ - and ^ are the only symbols allowed
4. Click **OK** to save the change.

Create Security Group Member dialog

Use the Create Security Group Member dialog, shown in [Figure 17](#), to add a member to a security group. Choose options from the Group Member (or manually enter a hex value) and **Authentication** drop-down lists, and enter values in the **Secret** and **Binding** (ISL groups only) fields.

Figure 17 Create a Security Group Member dialog

The conventions for ISL security group members are listed below:

- You can enter member World Wide Name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The authentication choices are None and CHAP (Challenge Handshake Authentication Protocol).
- The **Secret** field is disabled if authentication is set to None. If authentication is CHAP, the **Secret** field is enabled.
- **Generate** is only enabled when authentication is set to CHAP.
- Valid binding entries are 97–127.

The conventions for Port security group members are listed below:

- You can enter member World Wide Name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The authentication choices are None and CHAP.
- The **Secret** field is disabled if authentication is set to None. If authentication is CHAP, the **Secret** field is enabled.
- **Generate** is only enabled when authentication is set to CHAP.

The conventions for MS security group members are listed below:

- You can enter member World Wide Name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The CT (common transport) authentication choices are None, MD5, and SHA-1.
- The **Secret** field is disabled if authentication is set to None, otherwise the **Secret** field enabled.
- **Generate** is only enabled when authentication is CHAP.

- Secret is 16 byte length for MD5 authentication, and 20 bytes if authentication is SHA-1.

To add a member to a security group, perform the following procedure:

1. Choose one of the following to open the Edit Security dialog from the faceplate display:
 - Click **Security** on the tool bar.
 - Select **Security > Edit Security**.
2. Choose one of the following to open the Create a Security Group Member dialog:
 - Click a security group in the graphic window of the Edit Security dialog. Click **Security Member** in the tool bar.
 - Right-click on a security group in the graphic window of the Edit Security dialog. Select **Create Members** from the popup menu.
3. Open the **Group Member** drop-down list and select a Node World Wide Name. The switch must be a member of any group in which authentication is used. You can also enter a hex value.
4. Open the **Authentication** drop-down list, and select a type of protocol to be used for the authentication process for that member.
 - ISL authentication options are **None** (0 bytes), **CHAP** (16 bytes)
 - MS (CT — Common Transport) authentication options are **None** (0 bytes), **MD5** (16 bytes), **SHA** (20 bytes)
 - Port authentication options are **None** (0 bytes), **CHAP** (16 bytes)
5. Enter an authentication "password" to be assigned that member in the Secret area. Or, click **Generate** to randomly generate a secret.
6. Enter the domain ID (97–127) for the switch for the ISL group member in the **Binding** field (ISL groups only). The WWN of the switch must be at the entered domain ID when attempting to enter the fabric, otherwise it will become isolated.
7. Click **OK** to save the changes.

Editing the security configuration on a switch

To edit a security configuration on the switch from the faceplate display, perform the following procedure:

1. Choose one of the following to open the Edit Security dialog:
 - Click **Security** on the tool bar.
 - Select **Security > Edit Security**.

By default, the security configuration on the switch is displayed in the Edit Security dialog.
2. Choose one of the following from the Edit Security dialog:
 - Select **File > Open File**. Browse for and select the security file.
 - Press **Control+O** (letter o). Browse for and select the security file.
3. Click **Open** to display the security file in the Edit Security dialog.
4. Select the security item to edit in the graphic window, and choose one of the following:
 - **Rename a security set, or group**. Select a rename option from the Edit menu. Enter a new name in the Rename dialog. Click **OK** to save the changes.
 - **Edit security group member**. Select an **Edit Security Group Member** option from the Edit menu. Enter a new Group Member (WWN) in the Edit Security Group Member dialog. Choose an option in the **Authentication** drop-down list. Click **OK** to save the changes.
 - **Remove a security set, group, or member**. Select the item to remove, and select a remove option from the Edit menu. Click **OK** in the Remove dialog to remove that item from the security file and save the changes.
 - **Clear security**. Select the Security Sets directory name. Select **Edit > Clear Security**. Click **OK** in the Remove dialog to remove all security sets and save the changes. You can also right-click on the Security Sets (top level) directory name, select **Clear Security** from the popup menu, and click **OK** to remove all security sets.

5. To save the changes, choose one of the following:
 - Click **Apply** to save the changes and keep the Edit Security dialog open. Click **OK** to close the Edit Security dialog.
 - Click **OK** to save changes and close the Edit Security dialog.

Viewing properties of a security set, group, or member

To view the properties of a security set, group, or member from the faceplate display, perform the following procedure:

1. Click **Security** on the tool bar, or select **Security > Edit Security** to open the Edit Security dialog.
2. Choose one of the following:
 - Click a security set, security group, or security group member. Select **Edit > Properties**.
 - Right-click on a security item in the graphic window. Select **Properties** from the popup menu.
3. View the security information for the selected item in the Properties dialog.
4. Click **OK** to close the dialog.

Security Config dialog

Use the Security Config dialog, shown in [Figure 18](#), to save the active security configuration on the switch to non-volatile or to temporary memory, and to require the domain ID of a switch be validated before attaching to the fabric.

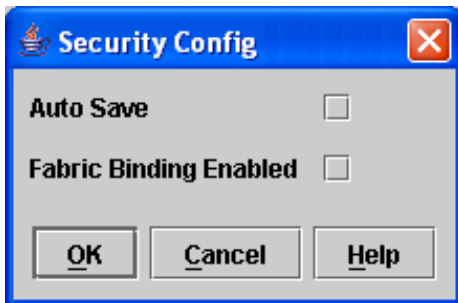


Figure 18 Security Config dialog

To configure switch security from the faceplate display, perform the following procedure:

1. Select **Security > Edit Security Config** to open the Security Config dialog.
2. Select the **Auto Save** option to enable (default) or disable Auto Save mode.

If enabled, the security configuration is saved to non-volatile memory on the switch. If disabled, the security file is saved only to temporary memory. The Auto Save feature is used when Fabric Binding is enabled. When Auto Save is disabled, any updates from remote switches will not be saved locally. If the local switch is reset, it may isolate.
3. Select the **Fabric Binding Enabled** option to require the expected domain ID of a switch to be verified before being allowed to attach to the fabric.



NOTE: The fabric binding feature must be enabled on all switches in the fabric. When enabling this feature, it is best to set the switch state to offline, enable the fabric binding feature on all switches, and then set the switch state to online.

4. Click **OK** to save the settings and close the Security Config dialog.

Archiving a security configuration to a file

To archive (save) a security configuration to a file from the faceplate display, perform the following procedure:

1. Click **Security** on the tool bar, or select **Security > Edit Security** to open the Edit Security dialog.
2. Make desired changes to the security settings using the security dialogs.
3. Select **File > Save As**.
4. Enter a name and location for the security file (.xml extension) in the Save dialog.
5. Click **Save** to save the security file.

Activating a security set

Only one security set can be active at one time. To activate a security set from the faceplate display, perform the following procedure:

1. Select **Security > Activate Security Set** to open the Activate Security Set dialog.
2. Select a security set from the drop-down list.
3. Click **Activate** to activate the security set.

Deactivating a security set

Only one security set can be active at one time. To deactivate an active security set from the faceplate display, perform the following procedure:

1. Select **Security > Deactivate Security Set**.
2. Select a security set from the drop-down list in the Deactivate Security Set dialog.
3. Click **Yes** to confirm that you want to deactivate the active security set in the Deactivate Security Set dialog.

Configured Security data window

The Configured Security data window displays a graphical representation of all security sets, security groups, and security group members in the database. Click the **Configured Security** data window tab in the faceplate display to open the Configured Security data window.

Active Security data window

The Active Security data window displays a graphical representation of the active security set, its groups, and members in the database. Click the **Active Security** data window tab in the faceplate display to open the Active Security data window.

Fabric services

Fabric services security includes SNMP and in-band management. Simple Network Management Protocol (SNMP) is the protocol governing network management and monitoring of network devices. SNMP security consists of a read community string and a write community string, that are basically the passwords that control read and write access to the switch. The read community string ("public") and write community string ("private") are set at the factory to these well-known defaults and should be changed if SNMP is enabled using the System Services or SNMP Properties dialogs. If SNMP is enabled (default) and the read and write community strings have not been changed from their defaults, you risk unwanted access to the switch. Refer to "[Enabling SNMP configuration](#)" on page 38 for more information. SNMP is enabled by default.

In-band management is the ability to manage switches across inter-switch links using McDATA Web Server, SNMP, management server, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than an Ethernet connection. Refer to "[Enabling in-band management](#)" on page 38 for more information.

Enabling SNMP configuration

To enable SNMP configuration from the faceplate display, perform the following procedure:

1. Select **Switch > SNMP Properties** to open the SNMP Properties dialog.
2. Select the **SNMP Enabled** option in the SNMP Configuration area.
3. Click **OK** to save the change to the database.

Enabling in-band management

To enable in-band management from the faceplate display, perform the following procedure:

1. Select **Switch > Switch Properties** to open the Switch Properties dialog.
2. Select the **In-band Management Enable** option.
3. Click **OK** to save the change to the database.

Tracking fabric firmware and software versions

The Fabric Tracker option enables you to generate a snapshot or baseline of current system version information, which can be viewed, analyzed and compared to other snapshot files, and exported to a file. Information includes date and time, McDATA Web Server version, switch active firmware version, device hardware, drivers, and firmware version from FDMI. Select **Fabric > Fabric Tracker** to open the Fabric Snapshot Analysis dialog shown in [Figure 19](#).

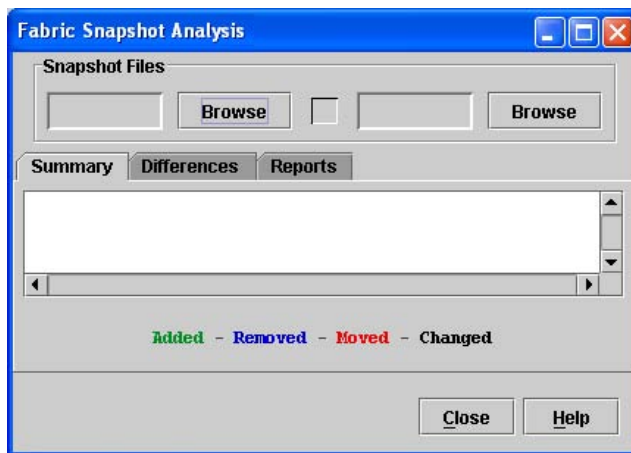


Figure 19 Fabric Snapshot Analysis dialog

Select **Fabric > Fabric Tracker > Analyze Snapshots** to view and analyze system version information. Use the **Analyze Snapshots** option to compare two snapshots, detect mismatches of firmware and driver versions, and detect devices that have been moved, added to or removed from the fabric.

The tab pages in the Fabric Snapshot Analysis dialog are:

- The Summary tab page shows a brief description of the changes that have occurred between the older snapshot and the newer one. Use the Summary tab page quickly view what has changed.
- The Differences tab page shows a side-by-side comparison of two snapshots.
- The Reports tab page enables you to select one of several reports to save to a text file.

Saving a version snapshot

The Fabric Snapshot Analysis dialog, shown in [Figure 19](#), opens with the Summary, Differences and Reports tab pages. Click **Browse** to open and view the snapshot files in the corresponding tab pages. Click **Close** to exit the Fabric Version Snapshot Analysis dialog. The color key below the scrollable area defines the meanings of the colors used. Select **Fabric > Fabric Tracker > Save Snapshot** to save the current snapshot to an XML file. Choose a pathname for the file in the Save dialog, and click **Save** to save the file.

Viewing and comparing version snapshots

The Differences tab page shows a side-by-side comparison of two snapshots. The timestamp of each snapshot is displayed above the scroll area showing that snapshot. The background color of the older snapshot is darker than the background of the newer snapshot. The arrow icon between the snapshot selectors always points from the older snapshot to the newer one. If the two snapshots have the same timestamp, the arrow will not be displayed. The scroll bars are synchronized to view the same portion of each snapshot file simultaneously. Click and drag the separator bar between the two panes to resize each pane. Click the left/right arrows at the top of the separator bar between the two panes to close the corresponding pane. The left/right arrows move to one side.

Exporting version snapshots to a file

The Reports tab page enables you to select one of several reports to save to a text file. There are two types of reports. The Summary report type shows the same format displayed on the Summary tab page without the color highlighting. The Detail report type shows a detailed breakdown of the differences. Click **Export** to save the selected report to a text file. Choose a pathname for the file in the Save dialog, and click **Save** to save the file.

Managing the fabric database

A fabric database contains the set of fabrics that you have added during a McDATA Web Server session. Initially, if you do not open an existing fabric or fabric view file, the McDATA Web Server application opens with an empty fabric database.

Adding a fabric

To add a fabric to the database, perform the following procedure:

1. Select **Fabric > Add Fabric** to open the Add a New Fabric dialog shown in [Figure 20](#).




Figure 20 Add a New Fabric dialog

2. Enter a fabric name (optional) and the IP address of the switch through which to manage the fabric.
3. Enter an account (login) name and password.

The factory account name and password are "admin" and "password". A password must have a minimum of 8 characters and no more than 20. The password is for the switch and is stored in the switch firmware. Refer to "[Managing user accounts](#)" on page 63 for information about creating user accounts.

4. Click **Add Fabric**.

-
-  **NOTE:** A switch supports a combined maximum of 19 logins or sessions as listed below:
- 4 logins or sessions for internal applications such as management server and SNMP
 - 9 high priority Telnet sessions
 - 6 McDATA Web Server and/or Telnet logins. Additional logins will be refused.
 - If the entry switch has SSL (Secure Socket Layer) enabled, the switch will generate and display a Verify Certificate dialog that you must accept before gaining access to the fabric. Refer to "[Connection security](#)" on page 30 and "[System Services dialog](#)" on page 80 for more information on certificates and SSL.
-

Removing a fabric

To delete a fabric file from the database, perform the following procedure:

1. Select a fabric in the fabric tree.
2. Select **Fabric > Remove Fabric**.

Opening a fabric view file

A fabric view file is one or more fabrics saved to a file. To open an existing view file, perform the following procedure:

1. Choose one of the following:
 - Select **Fabric > Add Fabric**
 - Click **Add** on the tool bar.
2. Enter a fabric name (optional) and the IP address of the switch through which to manage the fabric.
3. Enter an account (login) name and password. The factory account name and password are "admin" and "password". The password (8-20 characters) is for the switch and is stored in the switch firmware.
4. Click **Add Fabric**.

Rediscovering a fabric

After making changes to or deleting switches from a fabric view, it may be helpful to again view the actual fabric configuration. The rediscover fabric option clears out the current fabric information being displayed, and rediscovers all switch information. Select **Fabric > Rediscover Fabric** to rediscover a fabric. The rediscover function is more comprehensive than the refresh function.

Deleting switches and links

The McDATA Web Server application does not automatically delete switches or links that have failed or have been physically removed from the fabric. In these cases, you can delete switches and links to bring the display up to date. If you delete a switch or a link that is still active, the McDATA Web Server application will restore it automatically. You can also refresh the display. To delete a switch from the topology display, perform the following procedure:

1. Select one or more switches in the topology display.
2. Select **Switch > Delete**.

To delete a link, perform the following procedure:

1. Select one or more links in the topology display.
2. Select **Switch > Delete**.

Adding a new switch to a fabric

If there are no special conditions to be configured for the new switch, simply plug in the switch and the switch becomes functional with the default fabric configuration. The default fabric configuration settings are:

- Fabric zoning is sent to the switch from the fabric.
- External ports are 1-Gbps/2-Gbps/4-Gbps ports and are GL_Ports. Internal ports are 2-Gbps ports and are FL_Ports.
- The default static IP address of 10.0.0.1 and gateway of 10.0.0.254 are assigned to the switch without a gateway or boot protocol configured. Refer to ["IP configuration"](#) on page 82 for more information.

If you are adding a new switch to a fabric and do not want to accept the default fabric configuration, perform the following procedure:

1. If the switch is not new from the factory, reset the switch to the factory configuration before adding the switch to the fabric. Select **Switch > Restore Factory Defaults** from the faceplate display.
2. If you want to manage the switch through the Ethernet port, you must first configure the IP address using the Network Properties dialog or the Configuration Wizard. Refer to ["Network properties"](#) on page 82 and ["Using the configuration wizard"](#) on page 76 for more information.
3. Configure any special switch settings. Consider configuring the **Default Visibility** setting to **None** in the Zoning Config dialog to prevent devices from finding other devices on all switches in the fabric until the new switch is configured. Refer to ["Configuring the zoning database"](#) on page 54 for more information.
4. Plug in the inter-switch links (ISL), but do not connect the devices.
5. Configure the port types for the new switch using the Port Properties dialog. The 1-Gbps/2-Gbps/4-Gbps (external) ports can be G_Port, GL_Port, F_Port, or FL_Port. Refer to ["Configuring ports"](#) on page 100 for more information.
6. Connect the devices to the switch.
7. Make any necessary zoning changes using the Edit Zoning dialog. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog. Refer to ["Editing the zoning database"](#) on page 52 for more information.
8. If you changed the Default Visibility setting in the Zoning Config dialog from **All** to **None**, change that setting back to **All** if you want to allow devices connected to the switch to communicate when there is no active zoneset. If the McDATA 4Gb SAN Switch is in a fabric with other M-Series or McDATA directors or edge switches and there is no active zoneset, Default Visibility must be disabled (None) to avoid potential zoning incompatibilities. Select **Zoning > Edit Zoning Config** to open the Zoning Config dialog. Refer to ["Configuring the zoning database"](#) on page 54 for more information.

Replacing a failed switch

The archive/restore works for all switches. However, the Restore menu item is not available for the in-band switches. You can only restore a switch out-of-band (the fabric management switch). There are certain parameters that are not archived, and these are not restored by McDATA Web Server. Refer to ["Archiving a switch"](#) on page 85 and ["Restoring a switch"](#) on page 86 for information about archive and restore. Use the following procedure to replace a failed switch for which an archive is available.

1. At the failed switch:
 - a. Turn off the power.
 - b. Note the port locations and remove the interconnection cables and SFPs.
 - c. Remove the failed switch.
2. At the replacement switch:
 - a. Mount the switch in the location where the failed switch was removed.
 - b. Install the SFPs using the same ports as were used on the failed switch.

-
- △ **CAUTION:** Do not reconnect inter-switch links, target devices, and initiator devices at this time. Doing so could invalidate the fabric zoning configuration.
-

- c. Power up the switch.
3. Select the failed switch in the topology display. Select **Switch > Delete**.
4. Restore the configuration from the failed switch to the replacement switch:
 - a. Open a new fabric through the replacement switch. Refer to ["Adding a fabric"](#) on page 39 for more information.
 - b. Open the faceplate display for the replacement switch. Select **Switch > Restore**.
 - c. In the Restore dialog, enter the archive file from the failed switch or browse for the file.
 - d. Click **Restore**.
5. Reset the replacement switch to activate the configuration formerly possessed by the failed switch including the domain ID and the zoning database. Select **Switch > Reset Switch**. Refer to ["Resetting a switch"](#) on page 75 for more information.
6. Reconnect the inter-switch links, target devices, and initiator devices to the replacement switch using the same ports as were used on the failed switch.

Displaying fabric information

The topology display is your primary tool for monitoring a fabric. The graphic window of the topology display provides status information for switches, inter-switch links, and the Ethernet connection to the management workstation.

The data window tabs show device, switch, link, and active zone set information. The Active Zoneset data window shows the zone definitions for the active zone set. Refer to ["Devices data window"](#) on page 46 and ["Switch data window"](#) on page 68 for information about the Devices and Switch data windows.




Fabric status

The fabric updates the topology and faceplate displays by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the display status, or you can refresh the display at any time. To refresh the topology display, choose one of the following:

- Click **Refresh**.
- Select **View > Refresh**.
- Press **F5**.
- Right-click in the background of the topology display, and select **Refresh Fabric** from the popup menu.

The topology display uses switch and status icons to provide status information about switches, inter-switch links, and the Ethernet connection. The switch status icons, displayed on the left side of a switch, vary in shape and color. Switches controlled by an Ethernet Internet Protocol have a colored Ethernet icon displayed on the right side of the switch. A green Ethernet icon indicates normal operation, yellow indicates a condition that may require attention to maintain maximum performance, and red indicates a potential failure. [Table 4](#) shows the different switch icons and their meanings.

Table 4 Topology display switch and status icons


Switch icon	Description
	<p>McDATA 4Gb SAN Switch</p> <ul style="list-style-type: none"> • Normal operation (green) • Warning — operational with errors (yellow) • Critical — potential failure (red) • Unknown — communication status unknown, unreachable, or not manageable by the McDATA Web Server (blue)
	<p>Fabric management switch</p> <ul style="list-style-type: none"> • Ethernet connection normal (green) • Ethernet connection warning (yellow) • Ethernet connection critical (red)
	<p>Switch is not manageable with this version of McDATA Web Server. Use the management application that was shipped with this switch.</p>

Displaying the Event Browser

The Event Browser displays a list of events generated by the switches in the fabric and the switch management application. Events that are generated by the application are not saved on the switch, but can be saved to a file during the switch management session.

To display the Event Browser, choose one of the following:

- Select **Fabric > Show Event Browser**.
- Click **Events** on the tool bar.

 **NOTE:** If the Show Event Browser selection or the Events button is grayed-out, you must first enable the Events Browser using the Preferences dialog. Refer to "[Setting McDATA Web Server preferences](#)" on page 15 for more information. If the Event Browser is enabled using the Preferences dialog, the next time the switch management application is started, all events from the switch log will be displayed. If the Event Browser is disabled when switch management application is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

Entries in the Event Browser shown in [Figure 21](#) are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed in the Event Browser is 10,000. The maximum number of entries allowed on a switch is 1200. Once the maximum is reached, the event list wraps and the oldest events are discarded and replaced with the new events. Event entries from the switch, use the switch time stamp, while event entries generated by the application have a workstation time stamp. You can filter, sort, and export the contents of the Event Browser to a file. The Event Browser begins recording when enabled and switch management application is running.

Column sorting buttons

Severity column

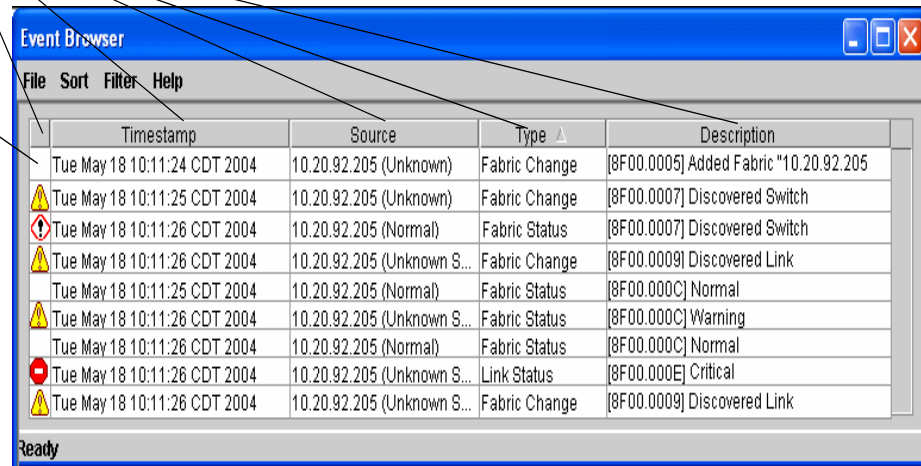





Figure 21 Event Browser

Severity is indicated in the severity column using icons as described in [Table 5](#).

Table 5 Severity levels

Severity icon	Description
	Alarm — an alarm is a "serviceable event". This means that attention by the user or field service is required. Alarms are posted asynchronously to the screen and cannot be turned off. If the alarm denotes that a system error has occurred the customer and/or field representative will generally be directed to provide a "show support" capture of the switch.
	Critical event — an event that indicates a potential failure. Critical log messages are events that warrant notice by the user. By default, these log messages will be posted to the screen. Critical log messages do not have alarm status as they require no immediate attention from a user or service representative.
	Warning event — an event that indicates errors or other conditions that may require attention to maintain maximum performance. Warning messages will not be posted to the screen unless the log is configured to do so. Warning messages are not disruptive and, therefore, do not meet the criteria of Critical. The user need not be informed asynchronously
No icon	Informative — an unclassified event that provides supporting information

NOTE: Events (alarms, critical, warning, and informative) generated by the application are not saved on the switch. They are permanently discarded when you close a McDATA Web Server session, but you can save these events to a file on the workstation before you close McDATA Web Server and read it later with a text editor or browser.

Events generated by the switch are stored on switch, and will be retrieved when the application is restarted. Some alarms are configurable. Refer to “[Configuring port threshold alarms](#)” on page 73.

Sorting the Event Browser

Sorting the Event Browser enables you to display the events in alphanumeric order based on the event severity, timestamp, source, type, or description. Initially, the Event Browser is sorted in ascending order by timestamp. Successive sort operations of the same type alternate between ascending and descending order. To sort the Event Browser, choose one of the following:

- Click the **Severity**, **Timestamp**, **Source**, **Type**, or **Description** columns.
- Select **Sort > By Severity**, **By Timestamp**, **By Source**, **By Type**, or **By Description**.

Filtering the Event Browser

Filtering the Event Browser enables you to display only those events that are of interest based on the event severity, timestamp, source, type, and description. Select **Filter > Filter Entries** in the Events Browser window to open the Filter Events dialog shown in [Figure 22](#). The Event Browser displays those events that meet all of the criteria in the Filter Events dialog. If the filtering criteria is cleared or changed, then all the events that were previously hidden that satisfy the new criteria will be shown.

You can filter the event browser the following ways:

- Severity — select one or more of the corresponding options to display alarm events, critical events, warning events, or informative events.
- Date/Time — select one or both of the **From:** and **To:** options. Enter the bounding timestamps (MM/dd/yy hh:mm:ss aa) to display only those events that fall within those times. ("aa" indicates AM or PM.) The current year (yy) can be entered as either 2 or 4 digits. For example, 12/12/03 will be interpreted December 12, 2003.
- Text — select one or more of the corresponding options and enter a text string (case sensitive) for event source, type, and description. The Event Browser displays only those events that satisfy all of the search specifications for the **Source**, **Type**, and **Description** text.

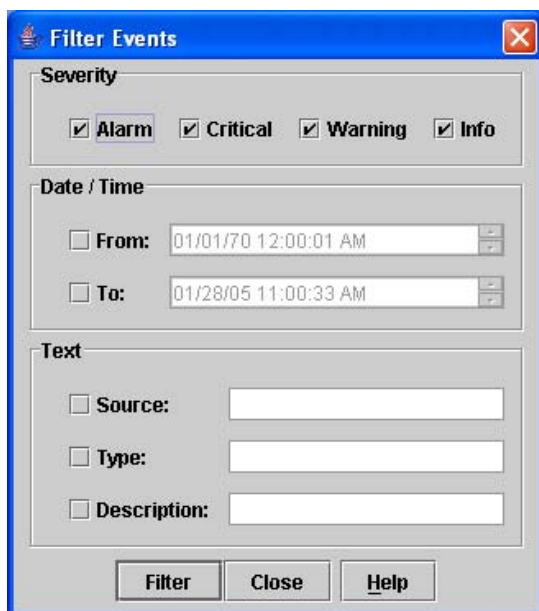


Figure 22 Filter Events dialog

Saving the Event Browser to a file

You can save the displayed Event Browser entries to a file. Filtering affects the save operation, because only displayed events are saved. To save the Event Browser to a file, perform the following procedure:

1. Filter and sort the Event Browser to obtain the desired display. Refer to ["Filtering the Event Browser"](#) on page 45 and ["Sorting the Event Browser"](#) on page 45 for more information.
2. Select **File > Save As**.
3. Select a pathname to which to save the event log and click **Save**. The file can be saved in XML, CSV, or text format. XML files can be opened with an internet browser or text editor. CSV files can be opened with most spreadsheet applications.

Devices data window

The Devices data window displays information about devices (hosts and storage targets) connected to the switch. Click the **Devices** data window tab, in either the topology or faceplate display, to display device information for all devices that are logged into the selected fabric. To narrow the display to devices that are logged into specific switches, select one or more switches in the fabric tree or the topology display. [Table 6](#) describes the entries in the Devices data window. Refer to ["Exporting device information to a file"](#) on page 48 for exporting device information.

Table 6 Devices data window entries

Entry	Description
Port WWN	Port World Wide Name
Nickname	Device port nickname. To create a new nickname or edit an existing nickname, double-click the cell and enter a nickname in the Edit Nickname dialog. Refer to "Managing device port nicknames" on page 48 for more information.
Details	Click (i) to display additional detail about the device. Refer to "Displaying detailed device information" on page 48.
FC Address	Fibre Channel address
Switch	Switch name
Port	Switch port number
Target/Initiator	Device type: target or initiator
Vendor	Host bus adapter/device vendor
Host Name	Name of host. This only applies to HBAs that support FDMI and register this data.
Active Zones	The active zone to which the device belongs
Row #	Row number reference for each listing in the Devices data window table

Active Zone Set data window

The Active Zoneset data window, shown in [Figure 23](#), shows the zone membership for the active zone set that resides on the fabric management switch. The active zone set is the same on all switches in the fabric – you can confirm this by adding a fabric through another switch and comparing Active Zone Set displays. Click the **Active Zoneset** data window tab in the topology display (only) to open the Active Zoneset data window. Refer to [“Configured Zonesets data windows”](#) on page 72 for information about the zone set definitions on a particular switch. Refer to [“Zoning a fabric”](#) on page 50 for more information about zone sets and zones.

The Active Zoneset data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its member ports/devices.
- Ports/devices that are zoned by WWN, but no longer part of the fabric, are grayed-out.

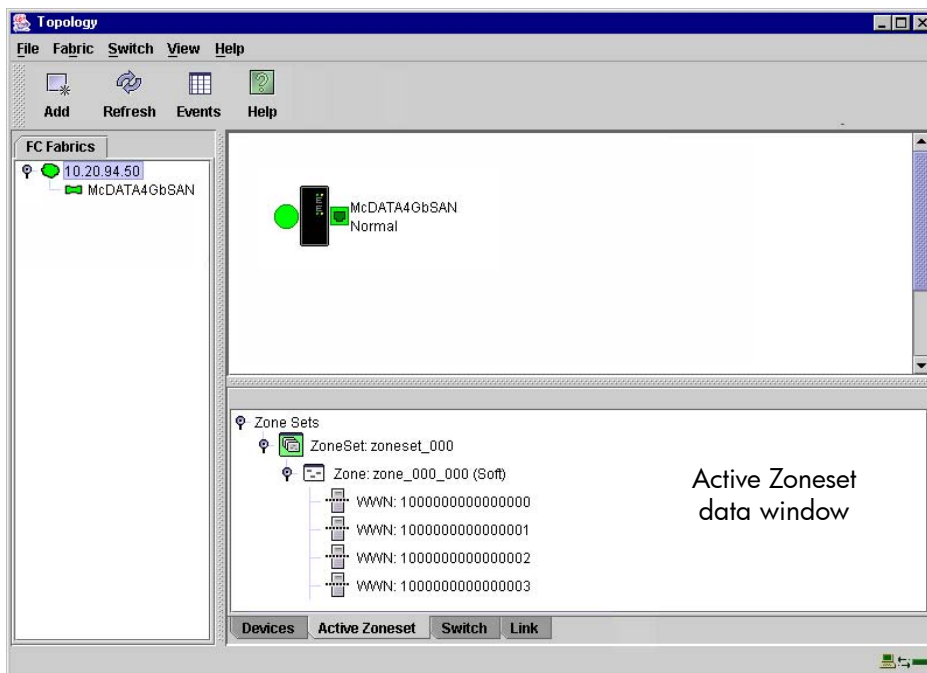


Figure 23 Active Zone Set data window

Link data window

The Link data window displays information about all switch links in the fabric or selected links. This information includes the switch name, the port number at the end of each link, and the link status icons. Click the **Link** data window tab in the topology display to open the Link data window.

Working with device information and nicknames

McDATA Web Server enables you to perform the following:

- Display detailed device information
- Export device information to a file
- Manage device port nicknames

Displaying detailed device information

In addition to the information that is available in the Devices data window, you can click (i) in the Details column to display more information as shown in Figure 24.

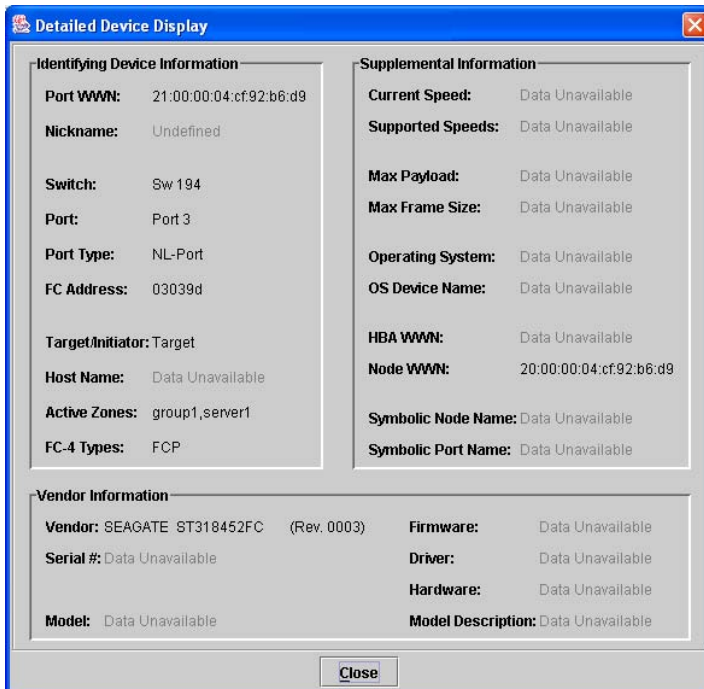


Figure 24 Detailed Device Display dialog

Exporting device information to a file

To save device information to a file, open the topology display and perform the following procedure:

1. Select one or more switches. If no switches are selected, devices information is gathered for all switches.
2. Select **Switch > Export Devices Information**.
3. Enter a file name in the Save dialog.
4. Click **Save**.

Managing device port nicknames

You can assign a nickname to a device port World Wide Name. A nickname is a user-definable, meaningful name that can be used in place of the World Wide Name. Assigning a nickname makes it easier to recognize device ports when zoning your fabric or when viewing the Devices data window.

McDATA Web Server maintains nicknames in the `Nicknames.xml` file, which is found in your working directory. In addition to creating, editing, and deleting nicknames, you can also export the nicknames to a file, which can then be imported into the `Nicknames.xml` file on other workstations.

Creating a nickname

To create a device port nickname, perform the following procedure:

1. Select **File > Nicknames** to open the Nicknames dialog.
2. Choose one of the following methods to enter a nickname. A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA—zZ][0—9] and special symbols [\$ _ - ^].
 - Click on a device in the table. Select **Edit > Create Nickname** to open the Add Nickname dialog. Enter a nickname and WWN and in the Add Nickname dialog. Click **OK**.
 - Double-click a cell in the **Nicknames** column. Enter a new nickname in the text field. Click **Save** to save the changes and exit the Nicknames dialog.
 - Double-click a cell in the Nickname column of the Devices data window. Refer to “[Devices data window](#)” on page 46.

Editing a nickname

A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA—zZ][0—9] and special symbols [\$ _ - ^]. You can access the Edit Nicknames dialog two ways. Choose one of the following to edit a nickname:

- Select **File > Nicknames** in the topology or faceplate display to open the Nicknames dialog. The device entries are listed in table format.
 - Click on a device entry in the table. Select **Edit > Edit Nickname** to open the Edit Nicknames dialog. Edit the nickname in the text field. Click **OK** to save the changes.
 - Double-click a cell in the **Nicknames** or **WWN** columns, and edit the nickname in the text field. Click **OK** to save the changes.
- Click the **Devices** data window tab in the topology or faceplate display to display the Devices data window. Double-click a cell in the **Nickname** column to open the Edit Nickname dialog. Edit the nickname in the text field. Click **OK** to save the changes. Refer to “[Devices data window](#)” on page 46 for more information.

Deleting a nickname

To delete a device port nickname, perform the following procedure:

1. Select **File > Nicknames** to open the Nicknames dialog
2. Click a device entry in the table.
3. Select **Edit > Delete Nickname**.
4. Click **Save** to save the changes.

Exporting nicknames to a file

You can save nicknames to a file. This is useful for distributing nicknames to other management workstations. To save nicknames to an XML file, perform the following procedure:

1. Select **File > Nicknames** to open the Nicknames dialog.
2. Select **File > Export** in the Nicknames dialog.
3. Enter a name for the XML nickname file in the Save dialog.
4. Click **Save**.

Importing a nicknames file

Importing a nicknames file copies its contents into and replaces the contents of the `Nicknames.xml` file which is used by McDATA Web Server. To import a nickname file, perform the following procedure:

1. Select **File > Nicknames** to open the Nicknames dialog.
2. Select **File > Import** in the Nicknames dialog.
3. Select an XML nickname file to import in the Open dialog.
4. Click **Open**.
5. Click **Yes** when prompted to overwrite existing nicknames.

Zoning a fabric

If EFCM or HAFM are used to manage the fabric, it is recommended to use EFCM or HAFM to manage the fabric zoning. If EFCM or HAFM are not used and other McDATA switch models are in the fabric, it is recommended to use SANpilot or Embedded Web Server to manage the fabric zoning. If all switches in the fabric are McDATA 4Gb SAN switches, use the zoning management of these switches as described in this manual. Zoning enables you to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes.

The McDATA 4Gb SAN Switch supports port/domain zoning in Standard/Open Fabric interop mode, other M-Series directors and edge switches do not. Therefore, only WWN zoning is supported in Standard/Open Fabric interop mode when McDATA 4Gb SAN Switch is attached to other McDATA switches. FC address zoning is not supported by other McDATA switches, and is not recommended for use in McDATA 4Gb SAN Switch.

This subsection addresses the following topics:

- [Zoning concepts](#), page 50
- [Managing the zoning database](#), page 52
- [Managing zone sets](#), page 56
- [Managing zones](#), page 58
- [Managing aliases](#), page 60
- [Merging fabrics and zoning](#), page 61

Zoning concepts

The following zoning concepts provide some context for the zoning tasks described in this section:

- [Zones](#), page 50
- [Aliases](#), page 50
- [Zone sets](#), page 51
- [Zoning database](#), page 51

Zones

A zone is a named group of ports, devices, or aliases that can communicate with each other. Membership in a zone can be defined by switch domain ID and port number, or device World Wide Name (WWN). Devices within a zone can only communicate with other devices in the same zone. Zones can overlap; that is, a device can participate in more than one zone. Zoning divides the fabric for purposes of controlling discovery. Devices within the same zone automatically discover and communicate freely with all other members of the same zone. The zone boundary is not secure; traffic across zones can occur if addressed correctly. Zones that include members from multiple switches need not include the ports of the inter-switch links.

- WWN entries define zone membership by the World Wide Name of the attached device. With this membership method, you can move WWN member devices to different switch ports in different zones without having to edit the member entry as you would with a domain ID/port number member. Furthermore, unlike FCID members, WWN zone members are not affected by changes in the fabric that could change the FC address of an attached device.
- Domain ID/Port number entries define zone membership by switch domain ID and port number. All devices attached to the specified port become members of the zone. The specified port must be an F_Port or an FL_Port.

Aliases

To make it easier to add a group of ports or devices to one or more zones, you can create an alias. An alias is a named set of ports or devices that are grouped together for convenience. Unlike zones, aliases impose no communication restrictions between its members. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias.

Zone sets


A zone set is a named group of zones. A zone can be a member of more than one zone set. Each switch in the fabric maintains its own zoning database containing one or more zone sets. This zoning database resides in non-volatile or permanent memory and is therefore retained after a reset. Refer to “[Configured Zonesets data windows](#)” on page 72 for information about displaying the zoning database.

The orphan zone set is created by the application automatically to hold the zones which are not in any set. The orphan zone set cannot be removed and is not saved on the switch.

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set. Refer to “[Active Zone Set data window](#)” on page 47 for information about displaying the active zone set.

Zoning database

Each switch has its own zoning database. The zoning database is made up of all aliases, zones, and zone sets that have been created on the switch or received from other switches. The switch maintains two copies of the inactive zoning database: one copy is maintained in temporary memory for editing purposes; the second copy is maintained in permanent memory. Zoning database edits are made on an individual switch basis and are not propagated to other switches in the fabric when saved. When a zone set is activated, it is propagated and saved to temporary memory in each switch in the fabric. If a switch has the Interop Auto Save parameter is enabled in the Zoning Config dialog, the zone set is saved to permanent memory on that switch.

 **NOTE:** If the Interop Auto Save parameter is enabled on the Zoning Configuration dialog, then every time the active zone set changes, the switch will copy it into an inactive zone set stored on the switch. You can edit this copy of the active zone set stored on the switch, and activate the updated copy to conveniently apply the changes to the active zone set. The edited copy then becomes the active zone set.

The configuration parameters affecting the zoning database are Interop Auto Save and Default Visibility. The Interop Auto Save parameter determines whether changes to the active zone set that a switch receives from another switch in the fabric will be saved to permanent memory on that switch. The Default Visibility parameter permits or prohibits communication among ports/devices when there is no active zone set. Refer to “[Configuring the zoning database](#)” on page 54 for information about zoning configuration.

Viewing zoning limits and properties

Zoning limits vary depending on the firmware installed on the switch. To view zoning limits and properties on a switch, perform the following procedure:

1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning dialog.
2. Choose one of the following:
 - Right-click on the top zonesets entry, a zone set, a zone, or a zone member in the zone sets tree (left windowpane). Select **Properties** in the popup menu.
 - select the top zonesets entry, a zone set, a zone, or a zone member in the zone set tree (left windowpane). Select **Edit > Properties**.
3. View the zoning limits and properties information in the Properties dialog.
4. Click **OK** to close the Properties dialog.

The zoning limits and definitions are:

- MaxZoneSets is 1. The maximum number of zone sets that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- MaxZones is 2000. The maximum number of zones that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.
- MaxAliases is 2500. The maximum number of aliases that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.

- MaxTotalMembers is 10,000. The maximum number of total zone and alias members that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Aliases are considered zone members since they can be added to a zone just like a normal zone member.
- MaxZonesInZoneSets is 2000. The maximum number of zone linkages to zonesets that can be configured on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Every time a zone is added to a zoneset this constitutes a linkage.
- MaxMembersPerZone is 2000. The maximum number of zone members that can be added to any zone on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric. Aliases are considered zone members when added to a zone.
- MaxMembersPerAlias is 2000. The maximum number of zone members that can be added to any alias on the switch. This will be enforced during the configuration of zoning and during a zoning database merge from the fabric.

Managing the zoning database

Managing the zoning database consists of the following:

- [Editing the zoning database](#), page 52
- [Configuring the zoning database](#), page 54
- [Saving the zoning database to a file](#), page 55
- [Restoring the zoning database from a file](#), page 55
- [Restoring the default zoning database](#), page 55
- [Removing all zoning definitions](#), page 56

Editing the zoning database

Select **Zoning > Edit Zoning** from the faceplate display to open the Edit Zoning dialog shown in [Figure 25](#). Changes can only be made to inactive zone sets, which are stored in flash (non-volatile) memory and retained after resetting a switch.

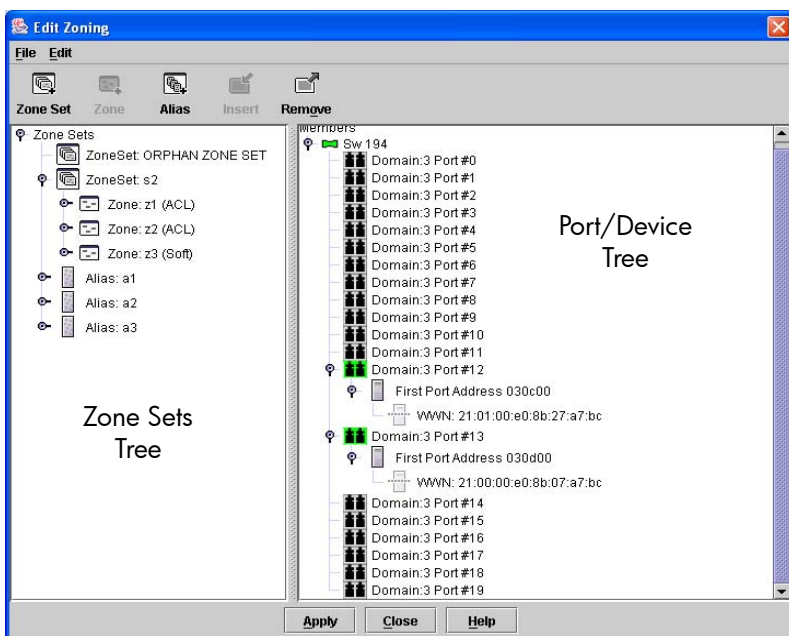



Figure 25 Edit Zoning dialog

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set.

You cannot edit an active zone set on a switch. You must configure an inactive zone set to your needs and then activate that updated zone set to apply the changes to the fabric. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric. However, in addition to the merged active zone set, each switch maintains its own original zone set in its zoning database. Only one zone set can be active at one time.

 **NOTE:** If the Interop Auto Save parameter is enabled on the Zoning Configuration dialog, then every time the active zone set changes, the switch will copy it into an inactive zone set stored on the switch. You can edit this copy of the active zone set stored on the switch, and activate the updated copy to conveniently apply the changes to the active zone set. The edited copy then becomes the active zone set.

The Edit Zoning dialog has a Zone Sets tree on the left and a Port/Device (or members) tree on the right. Both trees use display conventions similar to the fabric tree for expanding and contracting zone sets, zones, and ports. An expanded address shows the port World Wide Name.

You can select zone sets, zones, and ports in the following ways:

- Click a zone, zone set, or port icon.
- Right-click to select a zone set or zone, and open the corresponding popup menu.
- Press and hold **Shift** while clicking several consecutive icons.
- Press and hold **Control** while clicking several non-consecutive icons.

Using tool bar buttons, popup menus, or a drag-and-drop method, you can create and manage zone sets and zones in the zoning database. [Table 7](#) describes the zoning tool bar operations.

Use the Edit Zoning dialog to define zoning changes, and click **Apply** to open the Error Check dialog. Click **Error Check** to have McDATA Web Server check for zoning conflicts, such as empty zones, aliases, or zone sets. Click **Save Zoning** to implement the changes. Click **Close** to close the Error Check dialog. Click **Close** in the Edit Zoning dialog to close the Edit Zoning dialog.

Table 7 Edit Zoning dialog tool bar buttons and icons












Tool bar button	Description
 Zone Set	Create Zone Set button — create a new zone set
 Zone	Create Zone button — create a new zone
 Alias	Create Alias button — create another name for a set of objects
 Insert	Add Member button — adds selected port/device to a zone
 Remove	Remove Member button — delete the selected zone from a zone set, or delete the selected port/device from a zone
	Switch port icon — not logged in
	Switch port icon — logged in

Table 7 Edit Zoning dialog tool bar buttons and icons (continued)

Tool bar button	Description
	NL_Port (loop) device icon — logged in to fabric
	NL_Port (loop) device icon — not logged in to fabric
	N_Port device icon — logged in to fabric
	N_Port device icon — not logged in to fabric

Configuring the zoning database

Use the Zoning Config dialog to change the **Interop Auto Save**, **Default Visibility**, **Default Zone**, and **Discard Inactive** configuration parameters. Open the faceplate display. Select **Zoning > Edit Zoning Config** to open the Zoning Config dialog shown in [Figure 26](#). Click **OK** after making changes to put the new values into effect.

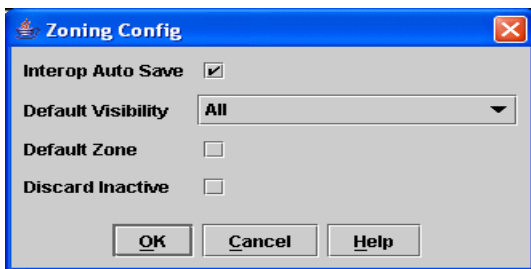



Figure 26 Zoning Config dialog

Interop Auto Save

The Interop Auto Save parameter determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to the zoning database on that switch. Changes are saved when an updated zone set is activated. Zoning changes are always saved to temporary memory. However, if Interop Auto Save is enabled, the switch firmware saves changes to the active zone set in temporary memory and to the zoning database. If Interop Auto Save is disabled, changes to the active zone set are stored only in temporary memory which is cleared when the switch is reset.

 **NOTE:** Disabling the Interop Auto Save parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Interop Auto Save parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Interop Auto Save parameter should be enabled in a production environment.

Default Visibility

The Default Visibility parameter is only applicable when the **Interop Mode** option on the Advanced Switch Properties dialog is set to Standard. The Default Visibility parameter determines the level of communication that is permitted between devices when there is no active zone set. It is recommended that all switches have the same Default Visibility setting. When default visibility is enabled (All, the default) on a switch, all ports on the switch can communicate with all ports on switches that also have Default Visibility enabled. When Default Visibility is disabled (None) on a switch, none of the ports on that switch can communicate with any other switch port in the fabric. The Default Visibility parameter permits or prohibits communication among ports/devices when there is no active zone set. If McDATA 4Gb SAN Switches are in a fabric with other M-Series directors and edge switches, and there is no active zone set, the Default Visibility parameter must be disabled (None) on the McDATA 4Gb SAN Switches, to avoid potential zoning incompatibilities.

Default Zone

The Default Zone parameter enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set or when there is no active zone set. This parameter must have the same value throughout the fabric. If interop mode is McDATA Fabric Mode, the Default Zone parameter is automatically distributed throughout the fabric. If McDATA 4Gb SAN Switches are in a fabric with other M-Series directors and edge switches, and the interop mode is Standard/Open Fabric, the Default Zone parameter MUST be disabled (False) on the McDATA 4Gb SAN Switches for zoning to function properly.

Discard Inactive

The Discard Inactive parameter automatically removes the previously active zone set when a zoneset is activated on a switch. The default setting is True.

Saving the zoning database to a file

You can save the zoning database to an XML file. You can later reload this zoning database on the same switch or another switch. To save a zoning database to a file, perform the following procedure:

1. Select **Zoning > Edit Zoning** in the faceplate display.
2. Select **File > Save As** In the Edit Zoning dialog.
3. Enter a file name for the database file in the Save dialog.
4. Click **Save** to save the zoning file.

Restoring the zoning database from a file

△ **CAUTION:** Restoring the zoning database from a file will replace the current zoning database on the switch.

To restore the zoning database from a file to a switch, perform the following procedure:

1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning window.
2. Select **File > Open File**. A popup window will prompt you to select an XML zoning database file.
3. Click **Open** after you select a file.

Restoring the default zoning database

Restoring the default zoning clears the switch of all zoning definitions. Restoring default zoning is a fabric-wide action. When you are in Standard mode and restore default zoning, no devices/ports are able to communicate with each other on the switches. When in McDATA mode, restoring default zoning, all devices/ports are able to communicate with each other if Default Zone is enabled, and no devices/ports are able to communicate with each other if Default Zone is disabled.

△ **CAUTION:** This command will deactivate the active zone set

To restore the default zoning for a switch, perform the following procedure:

1. Select **Zoning > Restore Default Zoning** in the faceplate display.
2. Click **OK** to confirm that you want to restore default zoning and save changes to the zoning database.

Removing all zoning definitions


To clear all zone and zone set definitions from the zoning database, select **Zoning > Edit Zoning** in the faceplate display and choose one of the following:

- Select **Edit > Clear Zoning**. Click **Yes** to confirm that you want to delete all zones and zone sets in the Removes All dialog.
- Right-click the Zone Sets heading at the top of the Zone Sets tree. Select **Clear Zoning** from the popup menu. Click **Yes** to confirm that you want to delete all zone sets and zones.

Managing zone sets

Zoning a fabric involves creating a zone set, creating zones as zone set members, then adding devices as zone members. The zoning database supports multiple zone sets to serve the different security and access needs of your storage area network, but only one zone set can be active at one time. Managing zone sets consists of the following tasks:

- [Creating a zone set](#), page 56
- [Activating and deactivating a zone set](#), page 57
- [Copying a zone to a zone set](#), page 57
- [Removing a zone from a zone set or from all zone sets](#), page 57
- [Removing a zone set](#), page 57

 **NOTE:** Zoning database edits are made on an individual switch basis and are not propagated to other switches in the fabric when saved. When a zone set is activated, it is propagated and saved to temporary memory in each McDATA 4Gb SAN Switch in the fabric. If a McDATA 4Gb SAN Switch has the Interop Auto Save parameter enabled in the Zoning Config dialog, the zone set is saved to permanent memory on that switch.

Creating a zone set

To create a zone set, perform the following procedure:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Select **Edit > Create Zone Set** to open the Create Zone Set dialog.
3. Enter a name for the new zone set, and click **OK**. The new zone set name is displayed in the Zone Sets dialog. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, -, ^, and \$.
4. To create new zones in the zone set, choose one of the following:
 - Right-click a zone set and select **Create A Zone** from the popup menu. In the Create a Zone dialog, enter a name for the new zone, and click **OK**. The new zone name is displayed in the Zone Sets dialog.
 - Copy an existing zone by dragging a zone into the new zone set. Refer to [“Copying a zone to a zone set”](#) on page 57.
5. Click **Apply** to save changes to the zoning database.

Activating and deactivating a zone set

You must activate a zone set to apply its zoning definitions to the fabric. Only one zone set can be active at one time. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every McDATA 4Gb SAN Switch in the fabric. To activate a zone set, perform the following procedure:

1. Select **Zoning > Activate Zone Set** to open the Activate Zone Set dialog.
2. Select a zone set from the **Select Zone Set** drop-down list.
3. Click **Activate** the selected zone set.

The purpose of the deactivate function is to suspend all fabric zoning which results in free communication fabric wide or no communication depending on the default visibility setting. Refer to "[Default Visibility](#)" on page 55 for more information. It is not necessary to deactivate the active zone set before activating a new one. To deactivate the active zone set, perform the following procedure:

1. Select **Zoning > Deactivate Zone Set** to open the Deactivate Zone Set dialog.
2. Acknowledge the warning about traffic disruption.
3. Click **Yes** to confirm that you want to deactivate the active zone set.

Copying a zone to a zone set

You can copy an existing zone and its membership from one zone set to another. Select the zone and drag it to the chosen zone set. Click **Apply** to save changes to the zoning database.

Removing a zone from a zone set or from all zone sets

To remove a zone from a zone set or from all zone sets in the database, perform the following procedure:

1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning dialog.
2. Select the zone or zones to be removed in the Zone Sets tree.
3. Select **Edit > Remove** to remove the zone from the zone set, or select **Edit > Remove from All Zones** to remove the zone from all zone sets.
4. Click **Apply** to save changes to the zoning database.

Alternatively, you can use shortcut menus to remove a zone from a zone set or from all zone sets in the database.

Removing a zone set

Removing a zone set from the database affects the member zones in the following ways.

- Member zones that are members of other zone sets are not affected.
- Member zones that are not members of other zone sets become members of the orphan zone set. The orphan zone set cannot be removed and is not saved on the switch.

To delete a zone set from the database, perform the following procedure:


1. Select **Zoning > Edit Zoning** in the faceplate display to open the Edit Zoning dialog.
2. Select the zone set to be removed in the Zone Sets tree.
3. Select **Edit > Remove** to remove the zone set.
4. Click **Apply** to save changes to the zoning database.

Alternatively, you may use shortcut menus to remove a zone set from the database.

Managing zones

Managing zones involves the following:


- [Creating a zone in a zone set](#), page 58
- [Adding zone members](#), page 58
- [Renaming a zone or a zone set](#), page 59
- [Removing a zone member](#), page 59
- [Removing a zone from a zone Set](#), page 59
- [Removing a zone from all zone sets](#), page 59

 **NOTE:** Changes you save to the zoning database on a switch are not propagated to other switches in the fabric unless you activate a zone set or edit the zoning databases on the individual switches in the fabric. When a zone set is activated, it is propagated and saved to temporary memory in each McDATA 4Gb SAN Switch in the fabric. If a switch has the Interop Auto Save parameter enabled in the Zoning Config dialog, the zone set is saved to permanent memory on that McDATA 4Gb SAN Switch. Refer to “[Configuring the zoning database](#)” on page 54 for more information.

Creating a zone in a zone set

To create a zone in a zone set, perform the following procedure:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Select a zone set in which to create a zone.
3. Select **Edit > Create a Zone**.
4. Enter a name for the new zone in the Create a Zone dialog
The new zone name is displayed in the Zone Sets dialog. A zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, ^, \$, and -.
5. Click **OK**.

 **NOTE:** If you enter the name of a zone that already exists in the database, the McDATA Web Server application will ask if you would like to add that zone and its membership to the zone set.

6. To add switch ports or attached devices to the zone, choose one of the following:
 - Select the zone set in the zone set tree. Select the port to add to the zone in the graphic window. Select **Edit > Add Members**.
 - Select a port by port number or World Wide Name in the Port/Device tree, and drag it into the zone.
 - Select a port by port number or World Wide Name in the Port/Device tree. Right-click the zone. Select **Add Zone Members** from the popup menu.
7. Click **Apply** to save changes to the zoning database.

Adding zone members


You can zone a port/device by switch domain ID and port number, or the device port WWN. Adding a port/device to a zone affects every zone set in which that zone is a member. Domain ID/port zoning is only supported in McDATA Fabric interop mode for other McDATA switches. To add ports/devices to a zone, perform the following procedure:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following methods to add the port/device:
 - Select a port/device in the Port/Device tree, and drag it into the zone. Press and hold **Control** while selecting multiple ports/devices.
 - Select a port/device in the Port/Device tree. Press and hold **Control** while selecting to select multiple ports/devices. Select a zone set in the left pane. Select **Edit > Add Members**.

- Select a port/device in the Port/Device tree. Press and hold **Control** while selecting multiple ports/devices. Select a zone set in the left pane. Click **Insert**.

If the port/device you want to add is not in the Port/Device tree, you can add it by doing the following:

- a. Right-click the selected zone.
 - b. Select **Edit > Create Members**.
 - c. Select the **WWN** or **Domain/Port** option.
 - d. Enter the hexadecimal value for the port/device according to the option selection: 16 digits for a WWN member, or 4 digits for a Domain/ Port member (DDPP).
3. Click **OK** to add the member and save the change.

 **NOTE:** Domain ID conflicts can result in automatic reassignment of switch domain IDs. These reassignments are not reflected in zones that use domain ID/port number pair to define their membership. Be sure to reconfigure zones that are affected by a domain ID change.

Renaming a zone or a zone set

To rename a zone, perform the following procedure:

1. Click the zone/zone set to be renamed in the Zone Sets tree of the Edit Zoning dialog.
2. Select **Edit > Rename**.
3. Enter a new name for the zone/zone set in the Rename Zone/Rename Zone Set dialog.
4. Click **OK** to save changes.

Removing a zone member

Removing a zone member will affect every zone and zone set in which that zone is a member. To remove a member from a zone, perform the following procedure:

1. Click the zone member to be removed in the Edit Zoning dialog.
2. Select **Edit > Remove**.
3. Click **OK** to save changes.

Removing a zone from a zone Set

The orphan zone set is created by the application automatically to hold the zones which are not in any set. The orphan zone set cannot be removed and is not saved on the switch. To remove a zone from a zone set, perform the following procedure:

1. Select the zone to be removed in the Edit Zoning dialog. The selected zone will be removed from that zone set only.
2. Select **Edit > Remove**.
3. Click **OK** to save changes.


Removing a zone from all zone sets

To remove a zone from all zone sets, perform the following procedure:

1. Select the zone to be removed in the Edit Zoning dialog.
2. Select **Edit > Remove Zone from All Sets**.
3. Click **OK** to save changes.

Managing aliases

An alias is a collection of objects that can be zoned together. An alias is not a zone, and cannot have a zone or another alias as a member.

 **NOTE:** Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches. You will not see aliases in the active zone set

Creating an alias

To create an alias, perform the following procedure:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Select **Edit > Create Alias** to open the Create Alias dialog.
3. Enter a name for the alias.
The alias name is displayed in the Zone Sets dialog. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, \$, ^, and -.
4. Click **OK** to close the Create Alias dialog.
5. Click **OK** to close the Edit Zoning dialog and save the alias name to the zoning database.

Adding a member to an alias

You can add a port/device to an alias by domain ID and port number, or the device port WWN. To add ports/devices to an alias, perform the following procedure:

1. Select **Zoning > Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following methods to add the port/device:
 - Select a port/device in the Port/Device tree, and drag it into the alias. Press and hold **Control** while selecting to select multiple ports/devices.
 - Select a port/device in the Port/Device tree. Press and hold **Control** to select multiple ports/devices. Select an alias. Select **Edit > Add Members**.
 - Select a port/device in the Port/Device tree. Press and hold **Control** while selecting to select multiple ports/devices. Select an alias. Click **Insert**.
3. If the port/device you want to add is not in the Port/Device tree, you can add it by doing the following:
 - a. Right-click the selected alias.
 - b. Select **Edit > Create Members**.
 - c. Choose the **WWN** or **Domain/Port** option.
 - d. Enter the hexadecimal value for the port/device according to the option selection: 16 digits for a WWN member or 4 digits for a Domain/ Port member (DDPP).
4. Click **OK** to add the member and save the change.

Removing an alias from all zones

To remove an alias from all zones, perform the following procedure:

1. Select the alias to be removed in the Zone Sets tree in the Edit Zoning dialog.
2. Select **Edit > Remove Alias from All Zones**.
3. Click **Yes** in the Remove dialog.

Merging fabrics and zoning


If you join two fabrics with an inter-switch link, the active zone sets from the two fabrics attempt to merge automatically. The fabrics may consist of a single switch or many switches already connected together. The switches in the two fabrics attempt to create a new active zone set containing the union of each fabric's active zone set. The propagation of zoning information only affects the active zone set, not the configured zone sets, unless Interop Auto Save is turned on.

Zone merge failure

If a zone merge is unsuccessful, the inter-switch links between the fabrics will isolate due to a zone merge failure, which will generate an alarm. The reason for the E_Port isolation can also be determined by viewing the port information. For more information, refer to "[Port Information data window](#)" on page 98, and "[Show command](#)" on page 178.

Zone merge failure recovery

When a zone merge failure occurs, the conflict that caused the failure must be resolved. You can correct a failure due to a zone conflict by deactivating one of the active zone sets or by editing the conflicting zones so that their membership is the same. You can deactivate the active zone set on one fabric if the active zone set on the other fabric accurately defines your zoning needs. If not, you must edit the zone memberships, and reactivate the zone sets. After correcting the zone membership, reset the isolated ports to allow the fabrics to join.

 **NOTE:** If you deactivate the active zone set in one fabric and the Interop Auto Save parameter is enabled, the active zone set from the second fabric will propagate to the first fabric and replace all zones with matching names in the configured zone sets.

Refer to "[Managing zones](#)" on page 58 for information about adding and removing zone members. Refer to "[Resetting a port](#)" on page 102 for information about resetting a port.

3 Managing switches

This section describes the following tasks that manage switches in the fabric.

- [Managing user accounts](#), page 63
- [Displaying switch information](#), page 68
- [Configuring port threshold alarms](#), page 73
- [Paging a switch](#), page 74
- [Setting the date/time and enabling NTP client](#), page 74
- [Resetting a switch](#), page 75
- [Configuring a switch](#), page 76
- [Archiving a switch](#), page 85
- [Restoring a switch](#), page 86
- [Restoring the factory default configuration](#), page 87
- [Downloading a support file](#), page 88
- [Installing firmware](#), page 89
- [Installing Product Feature Enablement \(PFE\) keys](#), page 88
- [Displaying hardware status](#), page 91

Managing user accounts

Only the Admin account can manage user accounts with the User Account Administration dialogs. However, any user can modify their own password. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.

A user account consists of the following:

- Account name or login
- Password
- Authority level
- Expiration date

Switches come from the factory with the following user accounts:


Table 8 Factory user accounts

Account name	Password	Admin authority	Expiration
admin	admin	true	never expires
images	images	false	never expires

The Admin account is the only user that can manage all user accounts with the User Account Administration dialogs. The Admin account can create, remove, or modify user accounts, and change account passwords. The Admin account can also view and modify the switch and its configuration with McDATA Web Server. The Admin account can not be removed.

Users with Admin authority can view and modify the switch and its configuration using McDATA Web Server. Users without Admin authority are limited to viewing switch status and configuration.

The Images account is used to exchange files with the switch using FTP. The Images account can not be removed.

 **NOTE:** If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

Creating user accounts

A switch can have a maximum of 15 user accounts. To create a new user account on a switch, perform the following procedure:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Add Account** tab to open the Add Account tab page shown in [Figure 27](#).
3. Enter an account name in the **New Account Login** field. Account names are limited to 15 characters.
4. Select the **Admin Authority Enabled** option if the account is to have the ability to modify switch configurations.
5. Enter a password in the **New Password** field and enter it again in the **Verify Password** field. A password must have a minimum of 8 characters and no more than 20.
6. Select the **Permanent Account** option if this account is to be permanent with no expiration date. Otherwise, select the **Account Will Expire** option and enter the number days in which the account will expire.
7. Click **Add Account** to add the newly defined account.
8. Click **Close** to close the User Account Administration dialog.



The screenshot shows the 'User Account Administration' dialog box with the 'Add Account' tab selected. At the top, there is a table listing existing accounts:

Login	Admin Authority	Days to Expiration
images	false	never expires
admin	true	never expires
rodtk	false	never expires
pats	true	never expires

Below the table, the 'Add Account' section contains the following fields and options:

- New Account Login:** A text input field.
- Admin Authority Enabled**
- New Password:** A text input field.
- Verify Password:** A text input field.
- Account Expiration Date:**
 - Permanent account (no expiration date)**
 - Account will expire in** **days (max of 2000 days)**

At the bottom of the dialog, there are several buttons: **Add Account**, **Remove Account**, **Change Password**, **Modify Account**, **Close**, and **Help**.

Figure 27 User Account Administration dialog — Add Account tab page

Removing a user account

To remove a user account on a switch, perform the following procedure:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Remove Account** tab to open the Remove Account tab page shown in [Figure 28](#).
3. Select the account (login) name from the list of accounts at the top of the dialog.
4. Click **Remove Account**.
5. Click **Close** to close the User Account Administration dialog.



Figure 28 User Account Administration dialog — Remove Account tab page

Changing a user account password

Any user can change their password for their account, but only the Admin account name can change the password for another user's account. If the administrator does not know the user's original password, the administrator must remove the account and add the account. To change the password for an account on a switch, perform the following procedure:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Change Password** tab to open the Change Password tab page shown in [Figure 29](#).
3. Select the account (login) name from the list of accounts at the top of the dialog.
4. Enter the old password, enter the new password, and re-enter the new password.
5. Click **Change Password**.
6. Click **Close** to close the User Account Administration dialog.



Figure 29 User Account Administration dialog — Change Password tab page

Modifying a user account

To modify a user account on a switch, perform the following procedure:

1. Select **Switch > User Accounts** in the faceplate display to open the User Account Administration dialog.
2. Click the **Modify Account** tab to open the Modify Account tab page shown in [Figure 30](#).
3. Select the account (login) name from the list of accounts at the top of the dialog.
4. Select the **Admin Authority Enabled** option to grant admin authority to the account name.
5. Select an **Account Expiration Date** option. If the account is not to be permanent, enter the number of days until the account expires.
6. Click **Modify Account** to save the changes.
7. Click **Close** to close the User Account Administration dialog.

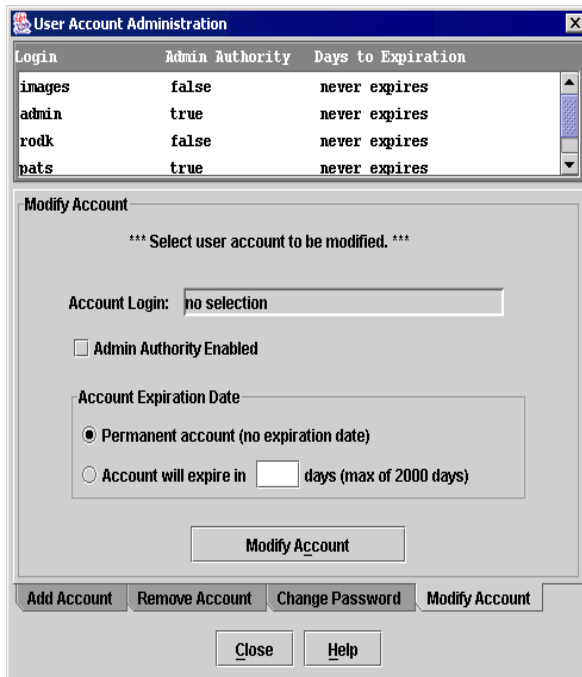


Figure 30 User Account Administration dialog — Modify Account tab page

Displaying switch information

The faceplate display and data windows provide the following switch information:

- Device and HBA information
- Switch specifications and addresses
- Configuration parameters
- Port performance statistics
- Port information
- Configured zone sets

Figure 31 shows the faceplate display for the McDATA 4Gb SAN Switch.

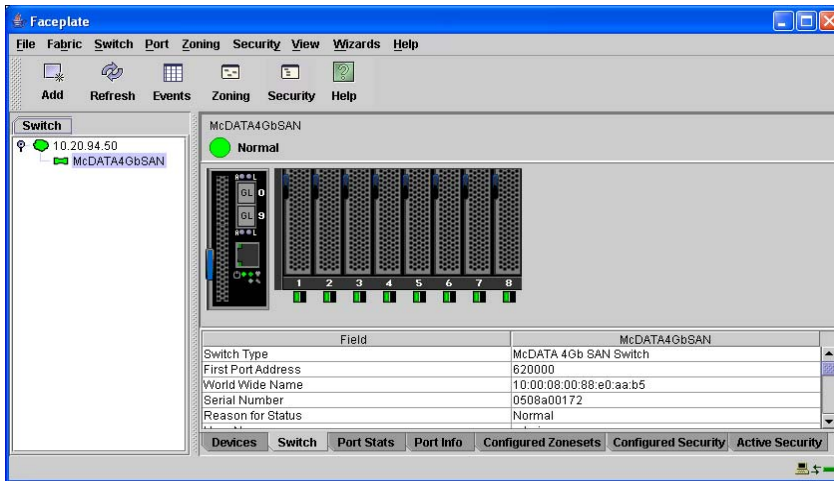


Figure 31 Faceplate display — switch information

The fabric updates the topology and faceplate displays by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the switch status, or you can refresh the display at any time. To refresh switch status in the display, choose one of the following:

- Click **Refresh**.
- Select **View > Refresh**.
- Press the **F5** key.
- Right-click a switch in the topology display. Select **Refresh Switch** from the popup menu.
- Right-click in the graphic window of the faceplate display. Select **Refresh Switch** from the popup menu.

Devices data window

The Devices data window displays information about devices (hosts and storage targets) connected to the switch. Click the **Devices** data window tab to display name server information for all devices that are logged into the selected fabric. To narrow the display to devices that are logged into specific switches, select one or more switches in the fabric tree or the topology display. Refer to “[Devices data window](#)” on page 46 for a description of the entries in the Devices data window.

Switch data window

The Switch data window displays current network and switch information for the selected switches. Refer to “[Configuring a switch](#)” on page 76 for more information about the Switch data window. [Table 9](#) describes the Switch data window entries.

To open the Switch data window, choose one of the following:

- Select one or more switches in the topology display. Click the **Switch** data window tab.
- Open the faceplate display. Click the **Switch** data window tab.

Table 9 Switch data window entries

Entry	Description
First Port Address	Switch FC address
World Wide Name	Switch World Wide Name
Serial Number	Number assigned to each chassis (required for PFE keys)
Reason for Status	Additional status information
User Name	Account name
Login Level	Authority level
Super User	Super user privileges enabled/disabled
UserAuthentication Enabled	Enforcement of account names and authority (always True)
Vendor	Switch manufacturer
Firmware Version	Active firmware version
Inactive Firmware Version	Not applicable
Pending Firmware Version	Firmware version that will be activated at the next reset
PROM/Boot Version	PROM boot version
MAC Address	Media Access Control address
IP Address	Internet Protocol address
Subnet Mask	Mask that determines the IP address subnet
Gateway	Gateway address
SNMP Enabled	SNMP enabled or disabled
Negotiated Domain ID	The domain ID currently being used by the fabric
Configured Domain ID	The domain ID defined by network administrator
Domain ID Lock	Domain ID lock status. Prevents (True) or permits (False—default) dynamic domain ID reassignment
Number of Ports	Number of ports activated on the switch
Operational State	Switch operational state: online, offline, diagnostic, down
Administrative State	Current switch administrative state
Configured Admin State	Switch administrative state that is stored in the switch configuration
R_A_TOV	Resource allocation timeout value
E_D_TOV	Error detect timeout value
Interop Mode	Interoperability mode. Use Standard to connect to FC-SW-2 compliant switches and McDATA switches in Open Fabric Mode. Use McDATA Fabric Mode to connect to McDATA switches in McDATA Fabric Mode. The default is Standard.
Legacy Address Format	Not applicable
Interop Auto Save	Zoning auto save status. Saves zoning updates in temporary memory and the zoning database (True), or only in temporary memory (False).

Table 9 Switch data window entries (continued)

Entry	Description
Zoning Default Visibility	Zoning visibility status. Permits (All) or prevents (None) communication between attached devices in the absence of an active zone set.
Default Zone	The Default Zone parameter enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set or when there is no active zone set. This parameter must have the same value throughout the fabric. If interop mode is McDATA Fabric Mode, the Default Zone parameter is automatically distributed throughout the fabric. If McDATA 4Gb SAN Switches are in a fabric with other M-Series directors and edge switches, and the interop mode is Standard/Open Fabric, the Default Zone parameter MUST be disabled (False) on the McDATA 4Gb SAN Switches for zoning to function properly.
Discard Inactive	Automatically removes the previously active zone set when a zoneset is activated on a switch
Temperature	Internal switch temperature °C
Security Auto Save	If enabled (default), the security configuration is saved to non-volatile memory on the switch. If disabled, the security file is saved only to temporary memory. The Auto Save feature is used when Fabric Binding is enabled. When Auto Save is disabled, any updates from remote switches will not be saved locally. If the local switch is reset, it may isolate.
Security Fabric Binding Enable	If enabled, the expected domain ID of a switch is required before attaching to the fabric
Fan 1 Status	Not applicable
Fan 2 Status	Not applicable
Power Supply 1 Status	Power supply 1 status
Power Supply 2 Status	Not applicable
Beacon Status	Beacon status. Switch LEDs are blinking (on) or not (off).
Broadcast Support	Broadcast support status. Broadcast support is enabled or disabled (default).
In-band Enabled	In-band management status. Permits (True) or prevents (False) a switch from being managed over a FC port.
Temperature Failure Port Shutdown	Non-configurable (always enabled for this switch). All ports are downed when the switch temperature exceeds the Failure Temperature.
Warning Temperature	Non-configurable temperature threshold (65° Celsius) above which a warning condition alarm is generated.
Failure Temperature	Non-configurable temperature threshold (70° Celsius) above which a failure condition alarm is generated.
NTP Client Enabled	Enabled or disabled. Allows for switches to synchronize their time a centralized server.

Table 9 Switch data window entries (continued)

Entry	Description
NTP Server Address	The IP address of the centralized NTP server. Ethernet connection to NTP server is required.
FDMI HBA Entry Limit	Maximum number of HBAs that can be registered with a switch.
FDMI Enable	Fabric Device Management Interface status. If enabled, device information can be obtained, managed, and saved through the fabric using Name Service Management Server functions. McDATA Web Server will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. Refer to "Displaying detailed device information" on page 48 for information about displaying FDMI information.
Embedded GUI	McDATA Web Server status. Enables or disables the web server on the switch.
Inactivity Timeout	Number of minutes the switch waits before terminating an idle CLI session. Zero (0) disables the time out threshold.
GUI Mgmt Enabled	Switch management application status. If disabled, the switch cannot be managed using the application.
Telnet Enabled	Telnet client status
SSH Enabled	Secure Shell status. If enabled, an encrypted data path is provided for CLI sessions.
SSL Enabled	Secure Sockets Layer status. If enabled, encryption for switch management application and CIM sessions is provided.
CIM Enabled	Common Information Model status. The CIM agent is based on the SNIA Storage Management Initiative Specification (SMI-S), which is the standard for SAN management in a heterogeneous environment.
FTP Enabled	FTP status
Management Server Enabled	Management server status

Port Statistics data window

The Port Statistics data window displays port performance data for the selected ports. Click the **Port Stats** data window tab in the faceplate display to open the Port Statistics data window. Refer to ["Port Statistics data window"](#) on page 96 for a description of the Port Statistics data window entries.

The **Statistics** drop-down list is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the drop-down list. Open the drop-down list and select **Absolute** to view the total count of statistics since the last switch reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. Click **Clear Baseline** to set the current baseline.

Port Information data window

The Port Information data window displays port detail information for the selected ports. Click the **Port Info** data window tab in the faceplate display to open the Port Statistics data window. Refer to ["Port Information data window"](#) on page 98 for a description of the Port Information data window entries.

Configured Zonesets data windows

The Configured Zonesets data window displays all zone sets, zones, aliases, and zone membership in the zoning database, shown in [Figure 32](#). Click the **Configured Zonesets** data window tab in the faceplate display to open the Configured Zonesets data window. Click the **Active Zonesets** data window tab in the topology display to view the active zone set in the Active Zonesets data window.

The Configured Zonesets data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle, located to the left of an entry in the tree, indicates the entry can be expanded. Click the entry handle, or double-click the following entries to expand or collapse them:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its members by device port World Wide Name, or device port FC address.
- The alias entry expands to show its entries.

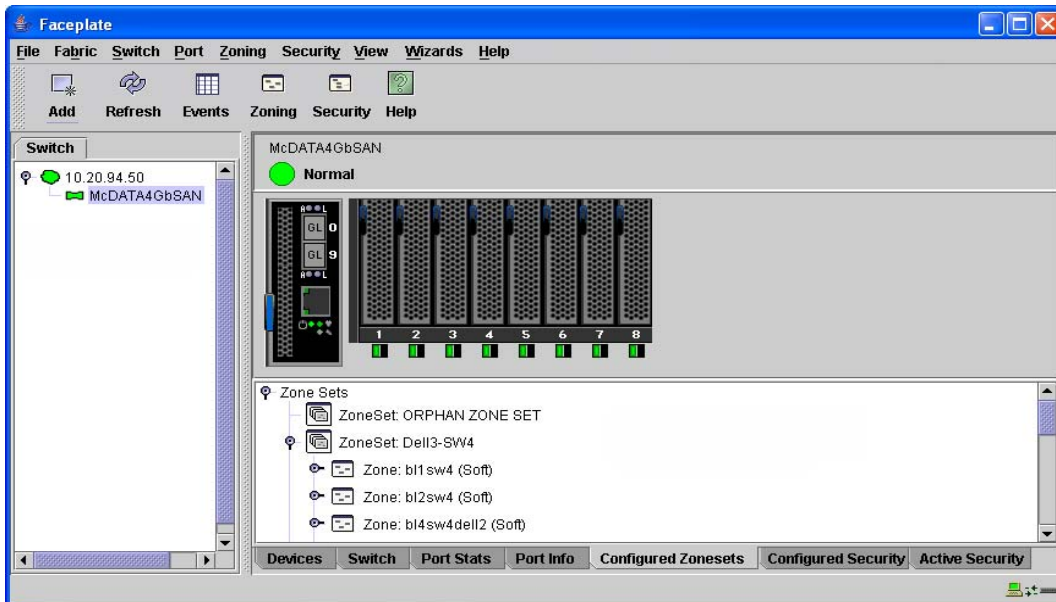


Figure 32 Configured Zonesets data window

Configuring port threshold alarms

You can configure the switch to generate alarms for selected events. Configuring an alarm involves choosing an event type, rising and falling triggers, a sample window, and finally enabling or disabling the alarm. To configure port threshold alarms, perform the following procedure:

1. Open the faceplate display.
2. Select **Switch > Port Threshold Alarm Configuration**. The Port Threshold Alarm Configuration dialog shown in [Figure 33](#) prompts you to enable or disable all alarms, select an event, set triggers, set a sample window and enable or disable an individual alarm.

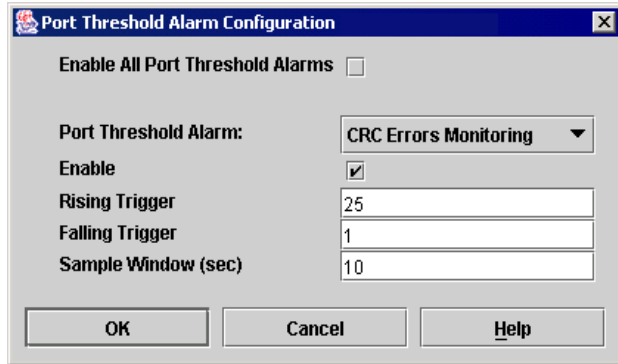


Figure 33 Port Threshold Alarm Configuration dialog

3. Select the **Enable All Port Threshold Alarms** option to enable monitoring for all the individual alarm types that are enabled. The **Enable All Port Threshold Alarms** option is the master control for the individual alarms. For example, the switch will monitor CRC errors only if both the **CRC Error Monitoring** option and the **Enable All Port Threshold Alarms** option are selected.
4. Select an event type from the **Port Threshold Alarm** drop-down list. Choose from the following options:
 - CRC error monitoring
 - Decode error monitoring
 - ISL monitoring
 - Device login monitoring
 - Device logout monitoring
 - Loss of signal monitoring
5. Select the **Enable** option to make the alarm eligible for use.
6. Enter a value for the rising trigger. A rising trigger alarm is generated when the event count per interval exceeds the rising trigger. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and rises again above the rising trigger. Consider the example in [Figure 34](#).
7. Enter a value for the falling trigger. A falling trigger alarm is generated when the event count per interval descends below the falling trigger.

NOTE: The switch will down a port if a rising trigger alarm is not cleared after three consecutive sample windows.

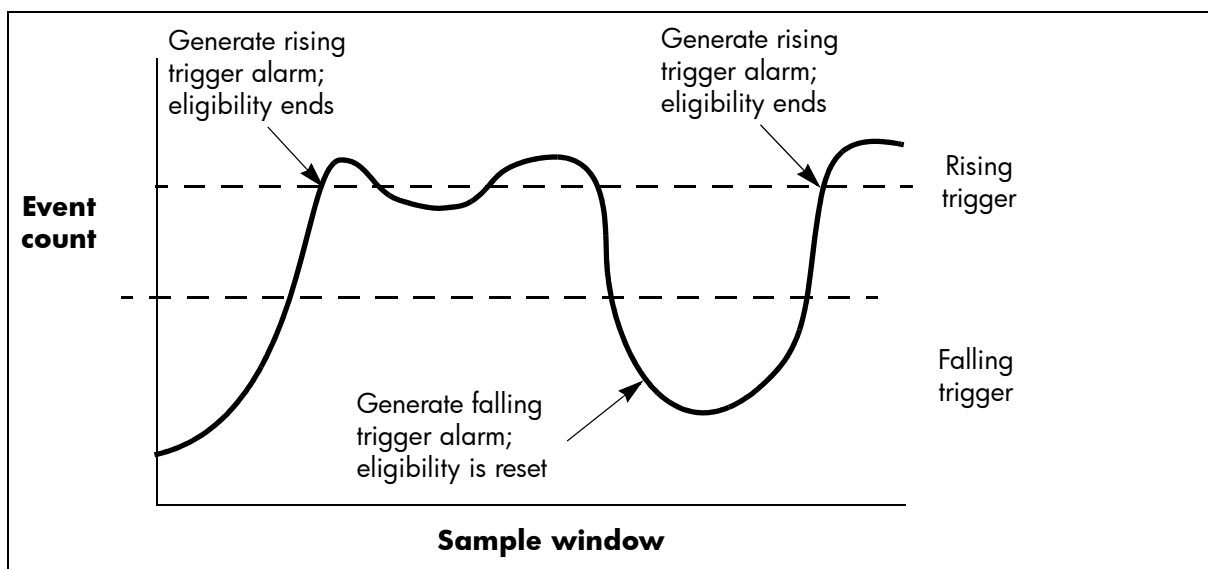


Figure 34 Port threshold alarm example

8. Enter a sample window in seconds. The sample window defines the period of time in which to count events.
9. Repeat steps 3 through 7 for each alarm you want to configure or enable.
10. Click **OK** to save all changes.

Paging a switch

You can use the beacon feature to page a switch. The beacon feature causes all Logged-In LEDs to flash, making it easier to recognize. Select **Switch > Toggle Beacon** (check mark shown) to page a switch. Select **Switch > Toggle Beacon** again (check mark removed) to cancel the beacon.

Setting the date/time and enabling NTP client

The Date/Time and Network Time Protocol (NTP) dialog enables you to manually set the date, time, and time zone on a switch, or to enable the NTP Client to synchronize the date, time, and time zone on the switch with an NTP server. Enabling the NTP client ensures the consistency of date and time stamps in alarms and log entries. An Ethernet connection to an NTP server is required. When date/time is set or displayed in the firmware, it is displayed based on the time zone configured. However, when displayed in the Date/Time dialog, the value is always in local time. The difference between switch and workstation times must not exceed 24 hours, or the switch management application can not connect. To set the date and time on a switch, perform the following procedure:

1. Select a switch in the topology display, and open the faceplate display.
2. Select **Switch > Set Date/Time**.
3. Choose one of the following:
 - Enter the year, month, day, time, and time zone in the Switch Date/Time dialog. Click **OK**. The new date and time take effect immediately.
 - Select the **NTP Client Enabled** option to enable the switch to synchronize its time with an NTP server. Enter the IP address of the NTP server. Ethernet connection to NTP server is required. Click **OK** to save the settings.

Resetting a switch

Resetting a switch reboots the switch using the switch configuration parameters last saved in permanent memory on the switch. Depending on the reset type, a switch reset may or may not include a Power On Self Test (POST) or it may or may not disrupt traffic. [Table 9](#) describes the types of switch resets.

During a hotreset operation, fabric services will be unavailable for a short period (30–75 seconds depending on switch model). Verify all administrative changes to the fabric (if any) are complete before performing an Non-Disruptive Code Load and Activation (NDCLA). When upgrading firmware across a fabric using non-disruptive activation, upgrade one switch at a time and allow 75 seconds between switches.

 **NOTE:** Changes to the fabric may disrupt the NDCLA process. More than one McDATA Web Server session will disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications
- Adding, moving or removing devices attached to the switch fabric — this includes powering up or powering down attached devices
- Adding, moving or removing ISLs or other connections

After an NDCLA operation is complete, management connections must be re-initiated:

- The McDATA Web Server session will re-connect automatically
- Telnet sessions must be restarted manually

Applicable code versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- An NDCLA operation to previous switch code releases is not supported

Table 10 Switch resets

Type	Description
Hot Reset	Resets a switch without a POST. This reset activates the pending firmware, but does not disrupt switch traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
Reset without POST	Resets a switch without a POST. This reset activates the pending firmware and it is disruptive to switch traffic.
Hard Reset	Resets a switch with a POST. This reset activates the pending firmware and it is disruptive to switch traffic.

To reset a switch using McDATA Web Server, perform the following procedure:

1. Select the switch to be reset and open the faceplate display.
2. Select **Switch > Reset Switch**:
 - Select **Hot Reset** to perform a hot reset
 - Select **Reset** to perform a standard reset
 - Select **Hard Reset** to perform a hard reset

Configuring a switch

Switch configuration is divided into three areas: chassis configuration, network configuration, and SNMP configuration. Chassis configuration specifies switch-wide FC settings. Network configuration specifies IP settings, remote logging, and the NTP client. SNMP configuration specifies SNMP settings and traps.

You can configure a switch explicitly or you can use the Configuration Wizard. The Configuration Wizard is a series of dialogs that guide you through the chassis, network, and SNMP configuration steps on new or replacement switches.

Using the configuration wizard

The Configuration Wizard is a series of dialogs you can use to configure the IP address and other basic parameters on new or replacement switches. McDATA Web Server will detect the first time use and present the Initial Start Dialog, from which the Configuration Wizard can be launched. Select **Wizards > Configuration Wizard** from either the topology display or the faceplate display to launch the Configuration Wizard. Use the Configuration Wizard to configure a new switch in a fabric.

Switch properties

To open the Switch Properties dialog, choose one of the following:

- Select a switch in the topology display. Select **Switch > Switch Properties**.
- Select **Switch > Switch Properties** in the faceplate display.
- Right-click a switch graphic in the topology display or faceplate display. Select **Switch Properties** from the popup menu.

Use the Switch Properties dialog to change the following switch configuration parameters:

- [Symbolic name](#), page 76
- [Switch administrative states](#), page 77
- [Domain ID and domain ID lock](#), page 77
- [Fabric Device Management Interface](#), page 78
- [Broadcast support](#), page 79
- [In-band management](#), page 79

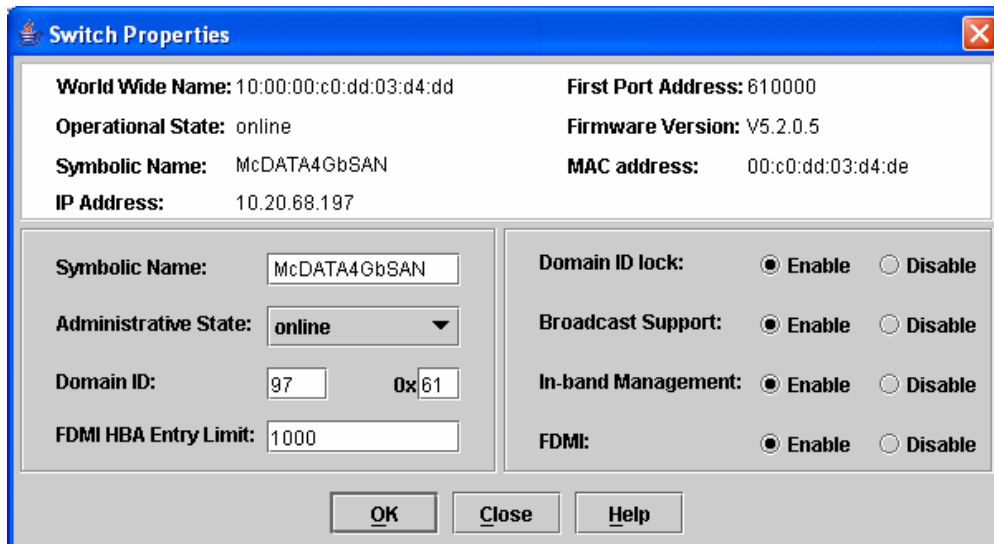


Figure 35 Switch Properties dialog

Symbolic name

The symbolic name is a user-defined name of up to 32 characters that identifies the switch. The symbolic name is used in the topology and faceplate displays, as well as many data windows to more easily identify switches. The illegal characters are the pound sign (#), semi-colon (;), and comma (,).

Switch administrative states

The switch administrative state determines the operational state of the switch. The switch administrative state exists in two forms: the configured administrative state and the current administrative state.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. McDATA Web Server always makes changes to the configured administrative state. The configured administrative state is displayed in the Switch Properties dialog.
- The current administrative state is the state that is applied to the switch for temporary purposes and is not retained across switch resets. The current administrative state is set using the Set Switch command. Refer to the “[Set command](#)” on page 154.

Table 11 describes the administrative state values.

Table 11 Switch administrative states


Parameter	Description
Online	The switch is available
Offline	The switch is unavailable
Diagnostics	The switch is in diagnostics mode, is unavailable, and tests can then be run on all ports of the switch. The switch must be reset after leaving the Diagnostics state.

Domain ID and domain ID lock

The domain ID is a unique value from 97–127 that identifies each switch in the fabric. The FC address consists of the domain ID, port ID, and the Arbitrated Loop Physical Address (ALPA). The maximum number of switches within a fabric is 31 with each switch having a unique domain ID.

Switches come from the factory with the Domain ID Lock setting disabled (False). This means that if there is a domain ID conflict in the fabric, the switch with the highest principal priority, or the principal switch, will reassign any domain ID conflicts and establish the fabric. If you lock the domain ID on a switch and a domain ID conflict occurs, one of the switches will isolate as a separate fabric and the Logged-In LEDs on both switches will flash to show the affected ports. Refer to the “[Set Config command](#)” on page 156 for information about the Switch keyword and the Domain ID Lock and Principal Priority parameters.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

 **NOTE:** Domain ID reassignment is not reflected in zoning that is defined by domain ID and port number pair. You must reconfigure zones that are affected by domain ID reassignment.

The McDATA 4Gb SAN Switch displays domain IDs differently in Standard mode than other M-series directors and edge switches. When the McDATA 4Gb SAN switch is in Standard mode (default), the domain ID will be displayed differently depending on which management utility is used. The valid Domain ID range while in standard mode is 97 (default) – 127. McDATA Web Server and CLI will display this as 97–127. EFCM/HAFM will display this as 1–31.

Prior to changing from Standard mode to McDATA Fabric mode, it is recommended that the switch be isolated from the fabric (take switch offline) before making the configuration changes and all domain IDs in the fabric should be noted to avoid conflicts. Once isolated, using CLI or McDATA Web Server, change interop mode to McDATA Fabric mode, and change the domain ID to a unique ID within the valid range of 1–31 for McDATA Fabric mode. It is then recommended that the Domain ID be locked to prevent conflict within the fabric. When all changes have been made and the switch has been brought back online, it should then be added into the fabric.

In McDATA Fabric mode, the McDATA 4Gb SAN Switch will display the domain IDs the same as other M-series directors and edge switches no matter which management utility is used. The valid domain ID range is 1–31 for McDATA Fabric mode.

Prior to changing from McDATA Fabric mode to Standard mode, it is recommended that the switch be isolated from the fabric (take switch offline) before making the configuration changes and all domain IDs in the fabric should be noted to avoid conflicts. Once isolated, using CLI or McDATA Web Server, change interop mode to Standard, and change the domain ID to a unique ID within the valid range of 97–127 for standard mode. It is then recommended that the Domain ID be locked to prevent conflict within the fabric. When all changes have been made and the switch has been brought back online, it should then be added into the fabric.

NOTE: Locking the domain ID prevents the principal switch from assigning a domain ID when the switch is added to the fabric. In a fabric where the principal switch is an M-series director or edge switch, this is not an issue. In a fabric where the McDATA 4Gb SAN Switch may be the principal switch, changing from McDATA Fabric mode to Standard mode without configuring the valid ID range and locking it, may result in the switch domain ID being converted to a number not within the valid range.

Table 12 lists the corresponding domain ID values for each interop mode: Standard mode and McDATA Fabric mode.

Table 12 Corresponding domain ID values by interop mode

McDATA Fabric mode	Standard mode	McDATA Fabric mode	Standard mode	McDATA Fabric mode	Standard mode
1	97	12	108	23	119
2	98	13	109	24	120
3	99	14	110	25	121
4	100	15	111	26	122
5	101	16	112	27	123
6	102	17	113	28	124
7	103	18	114	29	125
8	104	19	115	30	126
9	105	20	116	31	127
10	106	21	117		
11	107	22	118		

Fabric Device Management Interface

Fabric Device Management Interface (FDMI) provides a means to gather and display device information from the fabric, and allows FDMI capable devices to register certain information with the fabric, if FDMI is enabled. McDATA Web Server will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. To view FDMI data, FDMI must be enabled on the entry switch and on all other switches in the fabric which are to report FDMI data.

FDMI is comprised of the fabric-to-device interface and the application-to-fabric interface. The fabric-to-device interface enables a device’s management information to be registered. The application-to-fabric interface provides the framework by which an application obtains device information from the fabric. Use the **FDMI HBA Entry Limit** field on the Switch Properties dialog to configure the maximum number of HBAs that can be registered with a switch. If the number of HBAs exceeds the maximum number, the FDMI information for those HBAs can not be registered.

Use the **FDMI Enabled** option on the Switch Properties dialog to enable or disable FDMI. If FDMI is enabled on an HBA, the HBA forwards information about itself to the switch when the HBA logs into the switch. If FDMI is enabled on a switch, the switch stores the HBA information in its FDMI database. Disabling FDMI on a switch clears the FDMI database. If you disable FDMI on a switch and then re-enable it, you must reset the ports to cause the HBAs to log in again, and thus forward HBA information to the switch.

Click the **Devices** data window tab in the topology display and click **(i)** in the Details column of the Devices data window to view detailed FDMI information for a device. The Detailed Devices Display dialog displays the specific information for that device. Refer to “[Devices data window](#)” on page 46 for more information.

Broadcast support

Broadcast is supported on the switch and allows for TCP/IP support. Broadcast is implemented using the proposed standard specified in *Multi-Switch Broadcast for FC-SW-3, T11 Presentation Number T11/02-031v0*. Fabric Shortest Path First (FSPF) is used to set up a fabric spanning tree used in transmission of broadcast frames. Broadcast frames are retransmitted on all ISLs indicated in the spanning tree and all online N_Ports and NL_Ports. When a broadcast frame is received, these zones are enforced at the N_Ports and NL_Ports. If the originator of the broadcast is in a zone, the frame is retransmitted on all online N_Ports and NL_Ports within the zone. If the originator of the broadcast frame is not in a zone, the frame is retransmitted on online N_Ports and NL_Ports that are not in a zone. The default setting is disabled.

In-band management

In-band management is the ability to manage switches across inter-switch links using McDATA Web Server, SNMP, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than an Ethernet connection.

Advanced switch properties

The Advanced Switch Properties dialog enables you to set the timeout values and interop mode settings. The Advanced Switch Properties dialog is available for only the entry switch, because an in-band switch can not be taken offline. The switch will automatically be taken offline temporarily and will be restored to its original state after the changes are completed. Select **Switch > Advanced Switch Properties** to open the Advanced Switch Properties dialog. Click **OK** after making any changes to put the new values into effect. The default interop mode is Standard.

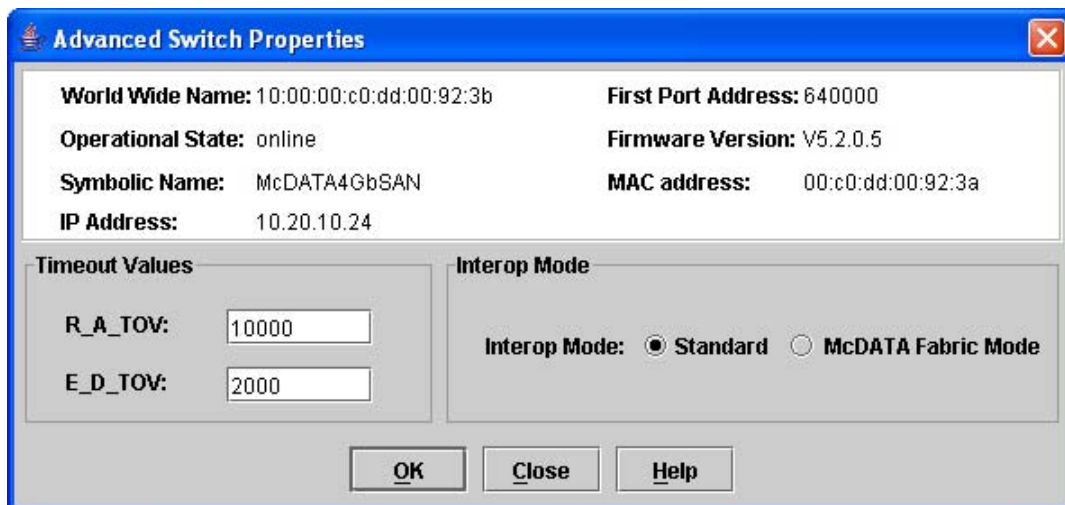


Figure 36 Advanced Switch Properties dialog

Timeout values

The switch timeout values determine the timeout values for all ports on the switch. [Table 13](#) describes the switch timeout parameters. The timeout values must be the same for all switches in the fabric.

NOTE: Mismatched timeout values will disrupt the fabric. These should not be changed unless absolutely necessary. Therefore, the switch must be offline to change these values. Use the Switch Properties dialog to take the switch offline.

Table 13 Timeout values

Parameter	Description
R_A_TOV	Resource Allocation Timeout — represents the maximum time a frame could be delayed in the Fabric and still be delivered. The default is 10000 milliseconds.
E_D_TOV	Error Detect Timeout — represents the maximum round trip time that an operation between two N_Ports could require. The default is 2000 milliseconds.

Interop mode for zoning

The interop mode permits interoperability with FC-SW-2 compliant and McDATA switches in McDATA Fabric Mode. The default interop mode is Standard.

- Use the **Standard** option to connect to FC-SW-2 compliant switches and McDATA switches in Open Fabric Mode.
- Use the **McDATA Fabric Mode** option to connect to McDATA switches in McDATA Fabric Mode.

System Services dialog

The System Services dialog provides a central location for you to enable or disable any of the external user services such as Simple Network Management Protocol (SNMP), Secure Sockets Layer (SSL), Secure SHell (SSH), embedded switch management application (McDATA Web Server), Command Line Interface (CLI), Network Time Protocol (NTP), and Common Information Model (CIM). Select **Switch > Services** to display the System Services dialog.

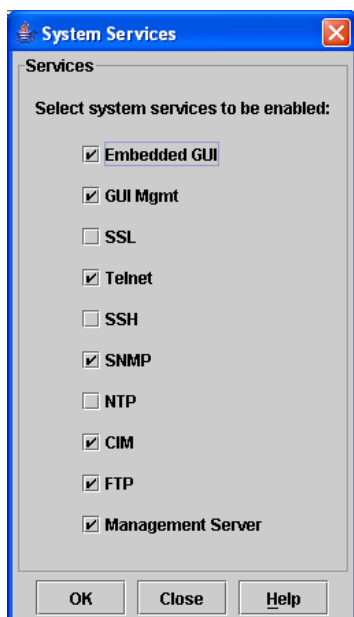


Figure 37 System Services dialog

△ **CAUTION:** Use caution when disabling the Embedded GUI (McDATA Web Server), GUI Mgmt, Telnet, SSL, and SSH, as it is possible to disable all access to the switch.

- **Embedded GUI** — McDATA Web Server. Allows users to point a browser at the switch and run the embedded switch management application on that switch as an applet.
- **GUI Mgmt** — allows out-of-band management of the switch from the switch management application (GUI). If disabled, the switch can not be specified as the entry switch for a fabric in the GUI, but can still be managed through an in-band connection.
- **SSL** — Secure Sockets Layer. Provides secure encrypted communications between the switch management application (GUI) and the switch. SSL must be enabled for configuration of security and RADIUS servers with the switch management application (GUI). SSL certificates are generated on the switch with the switch date/time and validated with the workstation's date/time. If the Switch and workstation date/time are not in sync, invalid certificates will be generated and prevent an SSL connection from being established between the switch and switch management application (GUI). To disable SSL when using a user authentication RADIUS server, the RADIUS authentication order must first be set to Local.
- **Telnet** — CLI. Allows users to manage the switch through a Telnet CLI session. Disabling Telnet access to the switch is not recommended.
- **SSH** — Secure SHell. Provides secure encrypted Telnet CLI sessions with the switch. Note that you will have to have an SSH client running on your workstation in order to manage your switch with Telnet CLI when SSH is enabled.
- **SNMP** — Simple Network Management Protocol. Allows management of the switch through third-party applications that use SNMP.
- **NTP** — Network Time Protocol. Allows the switch to obtain its time and date settings from an NTP server. Configuring all of your switches and your workstations to utilize NTP will keep their date/time settings in sync and will prevent difficulties with SSL certificates and event logs.
- **CIM** — Common Information Model. Allows management of the switch through third-party applications that use CIM.
- **FTP** — File Transfer Protocol. Allows file transfers to the switch via FTP. FTP is required for out-of-band firmware uploads which will complete faster than in-band firmware uploads.
- **Management Server** — allows management of the switch through third-party applications that use GS-3 Management Server.

Security Consistency Checklist dialog

The Security Consistency Checklist dialog enables you to compare security-related features on switches in order to check for inconsistencies. Any changes must be made through the appropriate dialog, such as Network Properties dialog, Switch Properties dialog, or SNMP Properties dialog. Select **Switch > Security Consistency Checklist** to open the Security Consistency Checklist dialog from the faceplate display.

Network properties

Use the Network Properties dialog shown in [Figure 38](#) to change IP configuration parameters and enable remote logging.

To open the Network Properties dialog, choose one of the following:

- Select a switch in the topology display. Select **Switch > Network Properties**.
- Open the faceplate display. Select **Switch > Network Properties**.

Click **OK** to put any new values into effect.

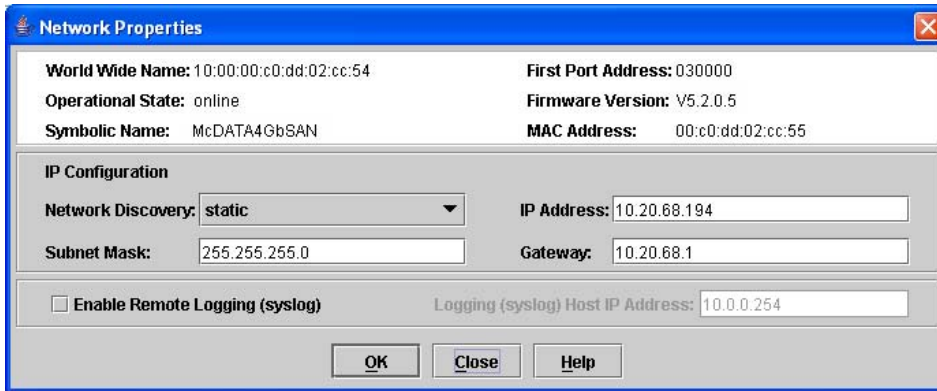


Figure 38 Network Properties dialog

IP configuration

The IP configuration identifies the switch on the Ethernet network and determines which network discovery method to use. [Table 14](#) describes the IP configuration parameters.

Table 14 IP configuration parameters

Parameter	Description
Network Discovery	<p>Choose one of the following options by which to assign the IP address:</p> <p>Static — uses the IP configuration parameters entered in the Switch Properties dialog</p> <p>BootP — acquires the IP configuration from a BootP server</p> <p>RARP (Reverse Address Resolution Protocol) — acquires the IP address from an RARP server. An RARP request is broadcast with up to three retries, each at 5 second intervals. If no IP address is obtained, the switch reverts to the previously configured IP address.</p> <p>DHCP (Dynamic Host Configuration Protocol) — acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch in order to avoid an IP address conflict. The DHCP server must then be made available.</p> <p>If a BootP, RARP, or DHCP server is not available, the switch will attempt to use a previously assigned valid lease. If no lease was ever assigned, the switch will attempt to use the previously assigned static IP address.</p>
IP Address	Internet Protocol (IP) address for the Ethernet port. The default value is 10.0.0.1.

Table 14 IP configuration parameters

Parameter	Description
Subnet mask	Subnet mask address for the Ethernet port. The default value is 255.0.0.0.
Gateway	IP gateway address. The default value is 10.0.0.254.

Remote logging

The Remote Logging (syslog) feature enables saving of the log information to a remote host that supports the syslog protocol. When enabled, the log entries are sent to the syslog host at the IP address that you specify in the **Logging Host IP Address** field. Log entries are saved in the internal switch log whether this feature is enabled or not.

To save log information to a remote host, you must edit the `syslog.conf` file (located on the remote host) and then restart the syslog daemon. Consult your operating system documentation for information on how to configure remote logging. The `syslog.conf` file on the remote host must contain an entry that specifies the name of the log file in which to save error messages. Add the following line to the `syslog.conf` file. A `<tab>` separates the selector field (`local0.info`) and action field which contains the log file path name (`/var/adm/messages/messages.name`).


```
local0.info <tab> /var/adm/messages.name
```

NTP client

The NTP Client feature allows switches to synchronize their date and time with a centralized server. NTP client ensures the consistency of date and time stamps in alarms and log entries. An Ethernet connection to NTP server is required. Refer to “[Setting the date/time and enabling NTP client](#)” on page 74 for more information.

SNMP properties

Use the SNMP Properties dialog shown in [Figure 39](#) to change SNMP configuration parameters. You must select a switch in the topology display or open the faceplate display to open the SNMP Properties dialog. Select **Switch > SNMP Properties**. Making any changes. Click **OK** to put the new values into effect.

 **NOTE:** Since read community, trap community, and write community settings are like passwords and are write-only fields, the current settings are displayed as asterisks.

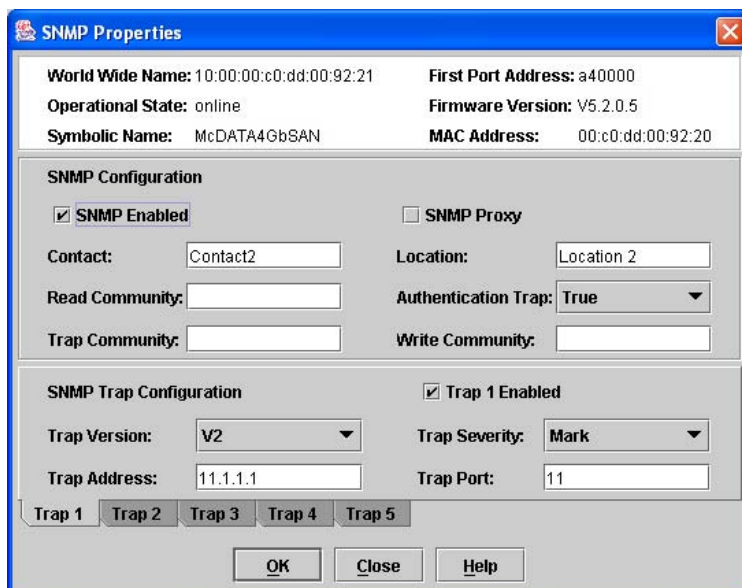


Figure 39 SNMP Properties dialog

SNMP configuration

The SNMP configuration defines how authentication traps are managed. [Table 15](#) describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 15 SNMP configuration parameters

Parameter	Description
SNMP Enabled	Enables or disables SNMP communication with other switches in the fabric
Contact	Specifies the name (up to 64 characters) of the person who is to be contacted to respond to trap events. The default is "undefined".
Read Community	Read community password (up to 32 characters) that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is "public".
Trap Community	Trap community password (up to 32 characters) that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is "public".
SNMP Proxy	If enabled, you can use SNMP to monitor and configure any switch in the fabric
Location	Specifies the name (up to 64 characters) for the switch location. The default is "undefined".
Authentication Trap	Enables or disables the reporting of SNMP authentication failures. If enabled, a notification trap is sent when incorrect community string values are used. The default value is "False".
Write Community	Write community password (up to 32 characters) that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is "private".

SNMP trap configuration

The SNMP trap configuration defines how traps are set. Choose from the tabs **Trap 1 – Trap 5** to configure each trap. [Table 16](#) describes the SNMP configuration parameters.

Table 16 SNMP trap configuration parameters

Parameter	Description
Trap Version	Specifies the SNMP version (1 or 2) with which to format traps
Trap 1 Enabled	Enables or disables the trap. If disabled, traps are not configurable.
Trap Address ¹	Specifies the IP address to which SNMP traps are sent. A maximum of 5 trap addresses are supported. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0.
Trap Port ¹	The port number on which the trap is sent. The default is 162.
Trap Severity	Specifies a severity level to assign to the trap. Open the drop-down list and choose a level. The Trap 1 Enabled option on the SNMP Properties dialog must be selected to access this drop-down list. Trap severity levels include Unknown, Emergency, Alert, Critical, Error, Warning, Notify, Info, Debug, and Mark

1. Trap address (other than 0.0.0.0) and trap port combinations must be unique. For example, if trap 1 and trap 2 have the same address, then they must have different port values. Similarly, if trap 1 and 2 have the same port value, they must have different addresses.

Archiving a switch

Archiving a switch saves the current switch configuration parameters to an .XML archive file containing the configuration parameters. Basically any data received by the application is archived. However, passwords are not archived with the user account information. The switch can later be restored using the saved switch configuration file. Archived parameters include switch properties and statistics, IP configuration, SNMP configuration, port properties and statistics, alarm configuration, and zoning configuration. Archived parameters include the following:

- Switch properties and statistics
- IP configuration
- SNMP configuration
- Port properties and statistics
- Alarm configuration
- Zoning configuration
- Configured security
- RADIUS Server information

This archive file can be used to restore the configuration on the same switch or on a replacement switch. You can also use the archive file as a template for configuring new switches to add to a fabric. The archive can be used later to restore the switch. Refer to [“Restoring a switch”](#) on page 86 for more information.

To archive a switch, perform the following procedure:

1. Select **Switch > Archive** in the faceplate display.
2. Enter a file name in the Save dialog.
3. Click **Save**.

Restoring a switch

Restoring a switch loads the archived switch configuration parameters to the switch. The switch configuration must be archived before it can be restored. The switch archive must be compatible with the switch to be restored; that is, you can restore a McDATA 4Gb SAN Switch only with an archive from a McDATA 4Gb SAN Switch. Refer to “[Archiving a switch](#)” on page 85 for more information.

NOTE: The switch being restored should be physically disconnected from the fabric. Restoring a switch in a fabric can severely disrupt the fabric. After the restore process is complete, the switch can be reconnected to the fabric.

The Restore dialog consists of the Full Restore tab page and Selective Restore tab page. To restore a switch, perform the following procedure:

1. Log in to the fabric through the switch you want to restore. You cannot restore a switch over an ISL.
2. Select **Switch > Restore** in the faceplate display to open the Restore dialog shown in [Figure 40](#).

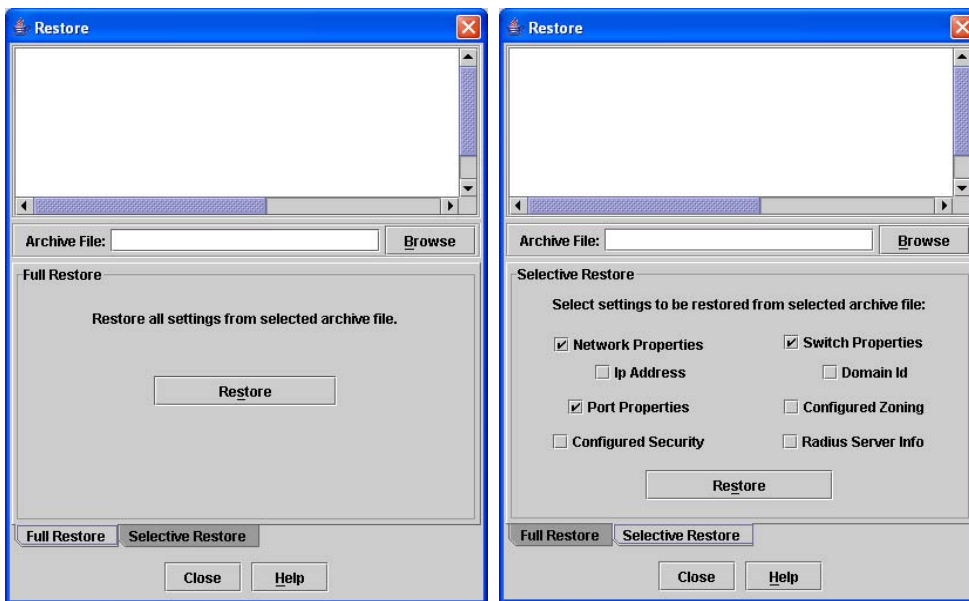


Figure 40 Restore dialogs – Full Restore and Selective Restore tab pages

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the McDATA Web Server Archive function. Configuration backup files created with the Config Backup command are not compatible with the McDATA Web Server Restore function.
4. Click the **Full Restore** tab.
5. Click **Restore** to restore all configuration settings.
6. Click the **Selective Restore** tab and select one or more of the following options. Click **Restore** to restore selected configuration settings:
 - **Network Properties** — restores all settings presented in the Network properties dialog except the IP address. Refer to [Network properties](#), page 82 for more information.
 - **IP Address** — restores switch IP address in addition to the other network properties. Refer to [IP configuration](#), page 82 for more information.
 - **Switch Properties** — restores all settings presented in the Switch properties dialog except the domain ID. Refer to [Switch properties](#), page 76 for more information.
 - **Domain ID** — restores switch domain ID in addition to the other switch properties. Refer to [Domain ID and domain ID lock](#), page 77 for more information.
 - **Port Properties** — restores all settings presented in the Port properties dialog. Refer to “[Configuring ports](#)” on page 100 for more information.

- **Configured Zoning** — restores all configured zone sets, zones, and aliases in the switch’s zoning database, excluding the active zone set. Refer to “[Configuring the zoning database](#)” on page 54 for more information.
 - **Configured Security** — restores all security sets in the switch database. Refer to “[Securing a fabric](#)” on page 30 for more information.
 - **Radius Server** — restores all RADIUS Server information defined in the switch database. Refer to “[RADIUS servers](#)” on page 25 for more information.
7. If you select the **Configured Zoning** or **Full Restore** option and the file contains zone sets, a dialog prompts you to activate one of those zone sets. Click **Yes**. Select a zone set from the drop-down list in the Select Zone Set to be Activated dialog.
 8. Click **OK** and view the results in the top pane of the Restore dialog.

Restoring the factory default configuration

You can restore the switch and port configuration settings to the factory default values. Select **Switch > Restore Factory Defaults** to restore the factory configuration on a switch. [Table 17](#) lists the factory default switch configuration settings. Restoring the switch to the factory default configuration does not restore the account name and password settings. The most current port license will remain in effect. To restore user accounts, you must select the **Reset Password File** option in the maintenance menu. Refer to “[Recovering a Switch Using Maintenance Mode](#)” in the *McDATA 4Gb SAN Switch for HP p-Class BladeSystem installation guide* for your switch for information about maintenance mode and the maintenance menu.

Table 17 Factory default configuration settings

Setting	Value
Symbolic Name	McDATA4GbSAN
Administrative State	Online
Domain ID	97
Domain ID Lock	False
In-band Management	True
Broadcast Support	Enable
Resource Allocation Timeout (R_A_TOV)	10000 milliseconds
Interop Mode	Standard
Device Scan Enabled	True
Error Detect Timeout (E_D_TOV)	2000 milliseconds
SNMP Enabled	True
SNMP Proxy	True
IP Address	10.0.0.1
FDMI Enabled	True
FDMI HBA Entry Level	1000
Subnet Mask Address	255.0.0.0
Gateway Address	10.0.0.254
Network Discovery	Static
Remote Logging	False
Remote Logging Host Ip Address	10.0.0.254
NTP Client Enabled	False

Table 17 Factory default configuration settings (continued)

Setting	Value
NTP Server IP Address	10.0.0.254
Contact	Undefined
Location	Undefined
Trap Enabled	False
Trap Port	162
Trap Address	Trap 1: 10.0.0.254; Traps 2-5: 0.0.0.0
Trap Community	Public
Read Community	Public
Write Community	Private
Port State	Online
Port Speed	Auto for external ports (0, 9) 2-Gbps for internal ports (1–8)
Port Type	External ports are GL_Ports Internal ports are FL_Ports

Downloading a support file


The **Download Support File** option assembles all log files and switch memory data into a core dump file (`dump_support.tgz`). This file can be sent to technical support personnel for troubleshooting switch problems. The menu option is not accessible (displayed) for switches that don't support the download support file function.

To create a support file, perform the following procedure:

1. Open the faceplate display.
2. Select **Switch > Download Support File**.
3. Click **Browse** to define a location for the support file or enter the path in the text field in the Download Support File dialog.
4. Click **Start** to begin the process of creating and downloading the support file to your workstation. Observe the status in the Status area.
5. Click **Close** to close the Download Support File dialog after the support file is saved to your workstation.

Installing Product Feature Enablement (PFE) keys

A Product Feature Enablement (PFE) key is a password that you can purchase from your switch distributor or authorized reseller to enable particular features in your switch. The SANtegrity Enhanced PFE key enables device security on the switch.

 **NOTE:** To obtain the McDATA 4Gb SAN Switch serial number and Product Feature Enablement key, follow the step-by-step instructions on the "firmware feature entitlement request certificate" for the PFE key. One of the license key retrieval options is via the web: www.webkey.external.hp.com.

To install a PFE key, perform the following procedure:

1. Add a fabric with the IP address of the switch on which you want to install the PFE key.
2. Open the faceplate display of the switch on which you want to install the PFE key.

3. Select **Switch > Features** to display the Feature Licenses dialog shown in [Figure 41](#).

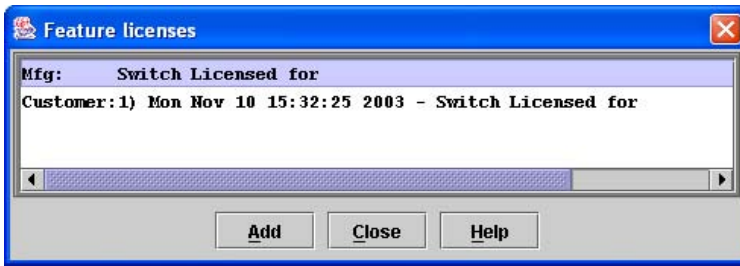


Figure 41 Features Licenses dialog

4. Click **Add** to open the Add License Key dialog shown in [Figure 42](#).

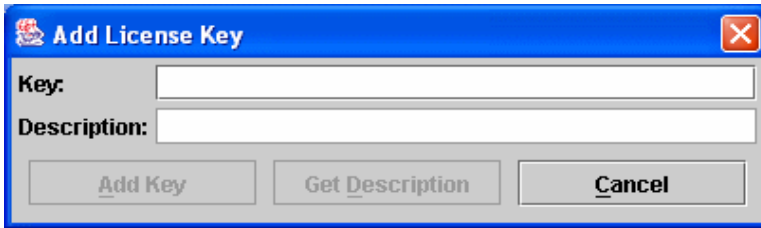


Figure 42 Add License Key dialog

5. Enter the license key in the **Key** field.
6. Click **Get Description** to display the PFE key description.
7. Click **Add Key**. Allow a minute or two to complete.

Installing firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management workstation as new firmware becomes available. You can use the McDATA Web Server application or the CLI to install new firmware.

You can load and activate firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the switch will perform a disruptive activation:

- The current firmware version is a version that supports upgrading to the new version
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes
- No port in the fabric is in the diagnostic state
- No zoning changes are being made in the fabric
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, McDATA Web Server sessions reconnect automatically. However, Telnet sessions must be restarted manually.

Using McDATA Web Server to install firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. McDATA Web Server does this in one operation. To provide consistent performance throughout the fabric, ensure that all McDATA 4Gb SAN Switch for HP p-Class BladeSystem switches are running the same version of firmware. Verify that this version of firmware is compatible with the firmware of other McDATA switch models in the fabric.

The pending firmware version will differ from the active version during the brief period while the switch is resetting to activate the firmware. Firmware management tools enable you to install and activate new firmware.

During a hotreset operation, fabric services will be unavailable for a short period (30-75 seconds). To ensure that an a Non-Disruptive Code Load and Activation (NDCLA) operation is successful, verify that all administrative changes to the fabric (if any) are complete. When you need to do NDCLA/hotreset to multiple switches, only perform the NDCLA/hotreset on one switch at a time, and allow a 75 second wait before performing the NDCLA/hotreset operation on the next switch.

△ **CAUTION:** Changes to the fabric may disrupt the NDCLA process. Common administrative operations that change the fabric include zoning modifications, adding, moving or removing devices attached to the switch fabric (this includes powering up or powering down attached devices), and adding, moving or removing ISLs or other connections.

To install firmware using McDATA Web Server, perform the following procedure:

1. Double-click a switch in the topology display to open the faceplate display.
2. Select **Switch > Load Firmware**.
3. Click **Browse**, and browse for and select the firmware file to be loaded in the Load Firmware dialog.
4. Click **Start** to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
5. Click **OK** to continue firmware installation, or click **Cancel** to cancel the firmware installation. McDATA Web Server will attempt a hot reset, if possible, to activate the firmware without disrupting data traffic. During a non-disruptive activation, all Logged-In LEDs are extinguished for several seconds. If a non-disruptive activation is not possible, an error message will be shown. To activate the firmware image, the user may either resolve the error described in the message and perform a hot reset on the switch or simply reset the switch (disruptive).

After an NDCLA operation is complete, management connections must be re-initiated:

- McDATA Web Server sessions will re-connect automatically
- Telnet sessions must be restarted manually

Applicable code versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- An NDCLA operation to previous switch code releases is not supported

Using the CLI to install firmware

To install firmware using the CLI when a File Transfer Protocol (FTP) server is present on the management workstation, use the Firmware Install command. Refer to the "[Firmware Install command](#)" on page 126 for more information. This command is disruptive to the fabric traffic.

1. Enter the following command to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware. If possible, a non-disruptive activation will be performed.

```
McDATA4GbSAN (admin) #> firmware install
```

```
Warning: Installing new firmware requires a switch reset. Continuing with this action will terminate all management sessions, including any Telnet sessions. When the firmware activation is complete, you may log in to the switch again.
```

```
Do you want to continue? [y/n]: y
```

```
Press 'q' and the ENTER key to abort this command.
```

2. Enter your account name on the remote host and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

```
User Account : johndoe
IP Address  : 10.20.20.200
Source Filename : 5.2.x.xx.xx_mpc
```

3. When prompted to install the new firmware, press **Y** to continue or press **N** to cancel. This is the last opportunity to cancel.

```
About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).

220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
```

4. Enter the password for your account name. The firmware will now be downloaded from the remote host to the switch, installed, and activated. The firmware is installed and the switch is automatically reset.

```
331 Password required for johndoe.
Password:*****
230 User johndoe logged in.

bin

200 Type set to I.

verbose

Verbose mode off.

This may take several seconds...

The switch will now reset.

Connection closed by foreign host.
```

Displaying hardware status

To display a summary of the hardware status information in a popup text box, rest the cursor over the chassis LED cluster in the faceplate display.

- Power LED — indicates the voltage status of the switch.
- Heartbeat LED — indicates the general status of the internal switch processor and the results of the POST.
- System Fault LED — indicates an error, such as an over temperature condition, internal system error, voltage fault, or corrupt configuration.



Figure 43 Hardware status LEDs


4 Managing ports

This section describes the following topics about managing ports and devices:

- [Displaying port information](#), page 93
- [Configuring ports](#), page 100
- [Resetting a port](#), page 102
- [Testing ports](#), page 102

Displaying port information

Port information is available primarily in the faceplate display shown in [Figure 44](#). The faceplate display data windows provide information and statistics for switches and ports. Use the topology display to view status information on fabrics, switches, and links between switches.

 **NOTE:** External ports are numbered 0 and 9; internal ports are numbered 1–8.

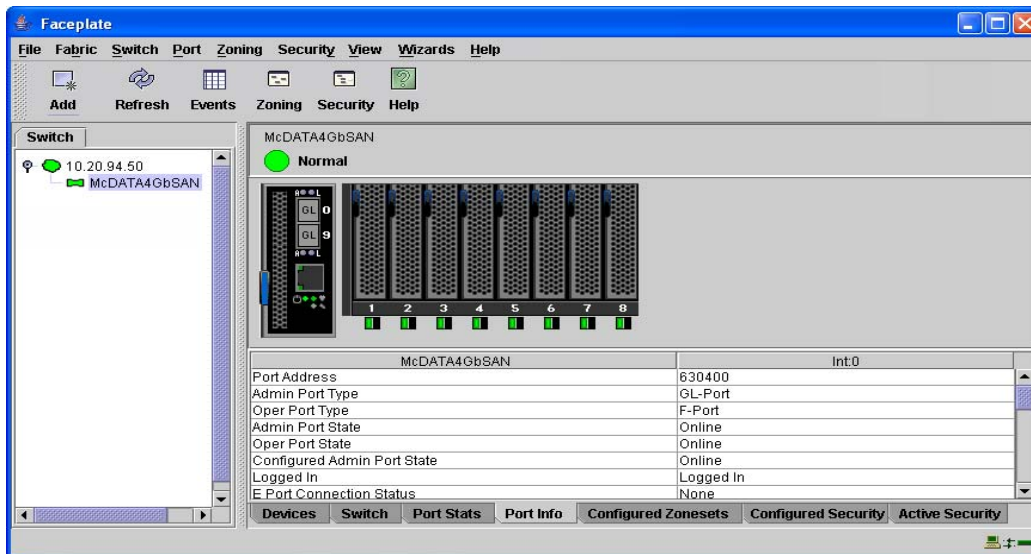


Figure 44 Faceplate display – port information

Monitoring port status

The faceplate display provides the following port related information:

- Port type
- Port operational state
- Port speed
- Port media

To display port number and status information for a port, position the cursor over a port on the faceplate display. The status information changes depending on the View menu option selected.

Displaying port types

To display port type status, from the faceplate display, select **View > View Port Types**. [Table 18](#) lists the possible port types and their meanings.

Table 18 Port types

State	Description
F_Port	Fabric port (point-to-point) — supports a single public device (N_Port)
FL_Port	Fabric loop port — self discovers a single device (N_Port) or a loop of up to 32 public devices (NL_Port). FL_Port is the default port type for internal ports
G_Port	Generic port — self discovers as an F_Port or an E_Port
GL_Port	Generic loop port — self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default port type for external ports. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port.
E_Port	Expansion port — the mode that a G_Port or GL_Port is in when attached by an ISL (inter-switch link) to another FC switch

Displaying port operational states

To display the operational state on each port in the faceplate display, select **View > View Port States**. [Table 19](#) lists the possible operational states and their meanings. The port operational state refers to actual port state and not the administrative state you may have assigned.

Table 19 Port operational states

State	Description
On	Online — port is active and ready to send data
la	Inactive — port operational state is offline, but administrative state is online
Iso	Isolated — E_Port has lost its connection. Refer to " Port Information data window " on page 98 for information about why the E_Port has isolated.
Off	Offline — port is active, can receive signal, but cannot accept a device login
Dia	Diagnostics — port is in diagnostics mode in preparation for testing
Dn	Down — the port is disabled, power is removed from the lasers, and can't be logged in

Displaying port speeds

To display the speed of each port in the faceplate display, select **View > View Port Speeds**. Table 20 lists the possible port speeds.





Table 20 Port speeds

State	Description
Au	Auto-detect
1Gb	1-Gbps transmission speed
2Gb	2-Gbps transmission speed
4Gb	4-Gbps transmission speed

Displaying transceiver media status

To display transceiver media status, select **View > View Port Media**. Table 21 lists the port media states and their meanings.

Table 21 Port transceiver media view

Media icon	Description
	Optical SFP, online (green)
	Optical SFP, offline (gray)
	Copper SFP, online (green)
	Copper SFP, offline (gray)
None	Empty port, no transceiver installed. This is normal for internal ports (1–8).

Port Statistics data window

The Port Statistics data window displays statistics about port performance. Select one or more ports in the faceplate display that you want to view statistics. Click the **Port Stats** data window tab to open the Port Statistics window. [Table 22](#) describes the Port Statistics data window entries.

The **Statistics** drop-down list is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the drop-down list. Open the drop-down list and select **Absolute** to view the total count of statistics since the last switch or port reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. Click **Clear Baseline** to set the current baseline when viewing baseline statistics. The baseline will also be set when the switch status changes from unreachable to reachable.

Table 22 Port Statistics data window entries

Entry	Description
Start Time	The beginning of the period over which the statistics apply. The start time for the Absolute view is not applicable. The start time for the Rate view is the beginning of polling interval. The start time for the Baseline view is the last time the baseline was set.
End Time	The last time the statistics were updated on the display
Total Time	Total time period from start time to end time
Al Init	Number of times the port entered the initialization state
AL Init Error	Number of times the port entered initialization and the initialization failed. Increments count when port has a sync loss
Bad Frames	Number of frames that were truncated due to a loss of sync or the frame didn't end with an EOF
Class 2 Frames In	Number of class 2 frames received by this port
Class 2 Frames Out	Number of class 2 frames transmitted by this port
Class 2 Words In	Number of class 2 words received by this port
Class 2 Words Out	Number of class 2 words transmitted by this port
Class 3 Frames In	Number of class 3 frames received by this port
Class 3 Frames Out	Number of class 3 frames transmitted by this port
Class 3 Toss	Number of class 3 frames that were discarded by this port. A frame can be discarded because of detection of a missing frame (based on SEQ_CNT), detection of an E_D_TOV timeout, receiving a reject frame, or receiving a frame on an offline port.
Class 3 Words In	Number of class 3 words received by this port
Class 3 Words Out	Number of class 3 words transmitted by this port
Decode Errors	Number of invalid transmission words detected during decoding. Decoding is from the 10-bit characters and special K characters.
Ep Connects	Number of E_Port logins
FBusy	Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_port that is preventing delivery of this frame.

Table 22 Port Statistics data window entries (continued)

Entry	Description
Flow Errors	Number of times a frame is received and all the switch ports receive buffers are full. The normal Fabric Login exchange of flow control credit should prevent this from occurring. The frame will be discarded.
FReject	Number of frames, from devices, that have been rejected. Frames can be rejected for any of a large number of reasons.
Invalid CRC	Number of invalid Cyclic Redundancy Check (CRC) frames detected
Invalid Destination Address	Number of address identifier (S_ID, D_ID) errors. AL_PA equals non-zero AL_PA found on F_Port.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
LIP (AL_PD,AL_PS)	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed
LIP(f7,AL_PS)	This LIP is used to re-initialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP(f7,f7)	A loop initialization primitive frame used to acquire an AL_PA
LIP(f8,AL_PS)	This LIP denotes a loop failure detected by the L_port identified by AL_PS
LIP(f8,f7)	A loop initialization primitive frame used to indicate that a Loop Failure has been detected at its receiver and does not have a valid AL_PA
Login Count	Number of device logins that have occurred on the switch
Logout Count	Number of device logouts that have occurred on the switch
Loop Timeouts	Number of loop timeouts
Loss Of Sync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
Primitive Sequence Errors	Number of bad primitives received by the port
Rx Link Resets	Number of link reset primitives received from an attached device
Rx Offline Sequences	Number of offline sequence primitives received by the port
Total Errors	Total number of primitive and non-primitive port link errors
Total Link Resets	Number of link-reset primitives transmitted and received by the port
Total LIPs Received	Number of loop initialization primitive frames received
Total LIPs Transmitted	Number of loop initialization primitive frames transmitted
Tx Offline Sequences	Number of offline primitives transmitted by the port

Table 22 Port Statistics data window entries (continued)

Entry	Description
Total Rx Frames	Total number of frames received by the port
Total Rx Words	Total number of words received by the port
Total Tx Frames	Total number of frames transmitted by the port
Total Tx Words	Total number of words transmitted by the port
Tx Link Resets	Number of link reset primitives sent from this port to an attached port
Total Offline Sequences	Total number of offline sequences transmitted and received by the port

Port Information data window

The Port Information data window displays detail information for the selected port. Click the **Port Info** data window tab in the faceplate display to open the Port Information data window.

Table 23 Port Information data window entries

Entry	Description
Port Address	Port FC address
Administrative Port Type	The administrative port type (G, GL, F, or FL). This value is persistent; it will be maintained during a switch reset. During port auto-configuration, it will be used to determine which operational port states are allowed.
Operational Port Type	The port type that is currently active. This will be set during port auto-configuration based on the administrative port type.
Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) which has been set by the user. This state may be different from the configured administrative state if the user has not saved it in the switch configuration. This state is used at the time it is set to try to set the port operational state. This value is not persistent and will be lost on a switch reset.
Operational Port State	The port state that is currently active. This value may be different from the administrative port state, for example due to an error condition.
Configured Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) which is saved in the switch configuration, either by the user or at the factory. This value is persistent; it will be maintained during a switch reset, and will be used after a reset to set the port operational state.
Logged In	Indicates whether logged in or not
E Port Connection Status	E_Port connection status. Status can be None, Connecting, Connected, or Isolated.
E Port Isolation Reason	Why E_Port is isolated

Table 23 Port Information data window entries (continued)

Entry	Description
MFS Mode	Multiple Frame Sequence bundling status
I/O Stream Guard	Not applicable
Administrative Port Speed	The speed requested by the user
Operational Port Speed	The speed actually being used by the port
Device Scan	Device scan status. Enabled means the switch queries the connected device during login for FC-4 descriptor information.
Symbolic Name	Port symbolic name
Media	The transceiver type
Media Speed	The maximum transceiver speed
Media Type	The transceiver fibre type, such as single mode, multi-mode, copper
Media Transmitter	The transceiver transmitter type, such as longwave, shortwave, electrical
Media Distance	The maximum transceiver transmission distance
Media Vendor	The company that manufactured the SFP
Media Vendor ID	The IEEE registered company ID
Media Part Number	The part number assigned to the SFP
Media Revision	Transceiver hardware version

Configuring ports

The port settings or characteristics are configured using the Port Properties dialogs shown in [Figure 45](#). Select a port in the faceplate display. Select **Port > Port Properties** to open the Port Properties dialog. The Port Properties dialog shows the switch name and the selected ports. Use the Port Properties dialogs to change the following parameters:

- Port state
- Port speed
- Port type
- Device scan

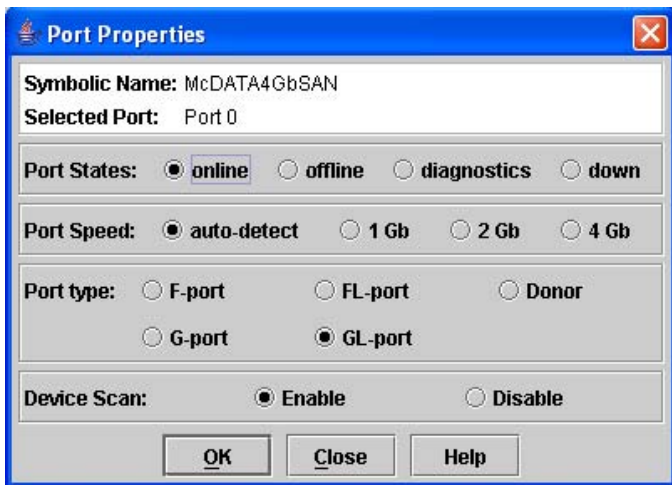


Figure 45 Port Properties dialog

Changing port administrative states

The port administrative state determines the operational state of a port. The port administrative state has two forms: the configured administrative state and the current administrative state.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. McDATA Web Server always makes changes to the configured administrative state.
- The current administrative state is the state that is applied to the port for temporary purposes and is not preserved across switch resets. The current administrative state is set using the Set Port command. Refer to the ["Set Port command"](#) on page 169.

[Table 24](#) describes the port administrative states. To change port administrative state, perform the following procedure:

1. Select one or more ports in the faceplate display.
2. Select **Port > Port Properties** to open the Port Properties dialog.
3. Select the option that corresponds to the port state you want.
4. Click **OK** to write the new port state to the switch.

Table 24 Port administrative states

State	Description
Online	Activates and prepares port to send data
Offline	Prevents port from receiving signal and accepting a device login
Diagnostics	Prepares port for testing and prevents the port from accepting a device login
Down	Disables the port

Changing port speeds

The 1-Gbps/2-Gbps/4-Gbps ports are capable of transmitting and receiving at 1-Gbps, 2-Gbps, or 4-Gbps. The ports can be configured for either transmission speed or to sense the transmission speed of the device to which it is connected. [Table 25](#) describes the port speeds. To change the port speed, perform the following procedure:

1. Select one or more 1-Gbps/2-Gbps/4-Gbps ports in the faceplate display.
2. Select **Port > Port Properties**.
3. Select the option that corresponds to the port speed you want.
4. Click **OK** to write the new port speed to the switch.

Table 25 Port speeds

State	Description
Auto-Detect	Matches the transmission speed of the connected device. This is the default.
1Gbps	Sets the transmission speed to 1-Gbps
2Gbps	Sets the transmission speed to 2-Gbps
4Gbps	Sets the transmission speed to 4-Gbps

Changing port types

The ports can be configured to self-discover the proper type to match the device or switch to which it is connected. [Table 26](#) describes the port types. To change the port type, perform the following procedure:

1. Select one or more ports in the faceplate display.
2. Select **Port > Port Properties**.
3. Select the option for the port type you want.
4. Click **OK** to write the new port type to the switch.

Table 26 Port types

State	Description
F_Port	Fabric port — supports a single public device (N_Port)
FL_Port	Fabric loop port — self discovers a single device (N_Port) or a loop of up to 32 public devices (NL_Port). The default internal port type.
G_Port	Generic port — self discovers as an F_Port or an E_Port
GL_Port	Generic loop port — self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default external port type. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port.

Device scan

The Device Scan feature queries the connected device during login for FC-4 descriptor information. Disable this parameter only if the scan creates a conflict with the connected device.

Changing port symbolic name

To change the symbolic name of a port from the faceplate display, perform the following procedure:

1. Open the faceplate display and select a port.
2. Select **Port > Port Symbolic Name**.
3. In the Port Symbolic Name dialog, choose one of the following:
 - Enter a new name for the port in the **Set Port Symbolic Name** field. The symbolic name can have up to 32 characters.
 - Select the **Restore Default Port Symbolic Name** option to restore the default name.
4. Click **OK**.

Resetting a port

The **Reset Port** option re-initializes the port using the saved configuration. To reset a port, perform the following procedure:

1. Select the port(s) to be reset in the faceplate display.
2. Select **Port > Reset Port**.

Testing ports

The port loopback tests verify correct port operation by sending a frame out through the loopback, and then verifying that the frame received matches the frame that was sent. Only one port can be tested at a time for each type of test. The Port Loopback Test dialog shown in [Figure 46](#) presents the following loopback tests:

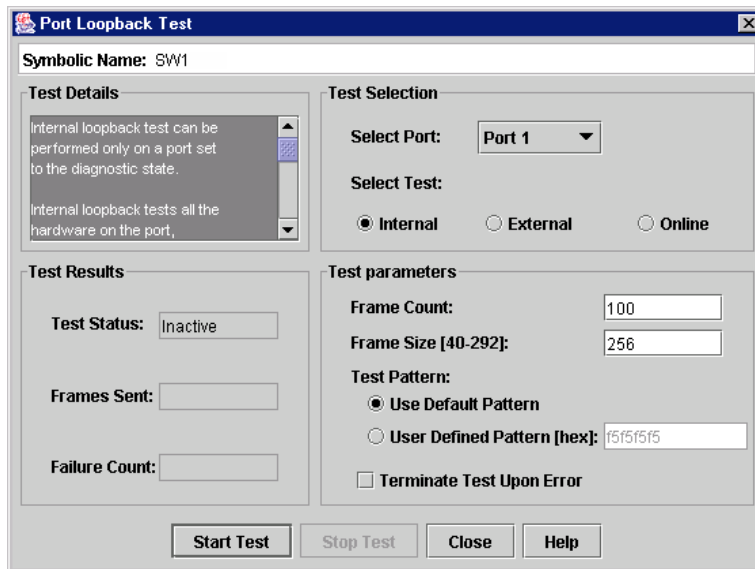


Figure 46 Port Loopback Test dialog

- **SerDes level (internal)** — the SerDes level test verifies port circuitry. The SerDes level test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.
- **SFP level (external)** — the SFP level test verifies port circuitry. The SFP level test sends a test frame from the ASIC through the SerDes chip, through the SFP transceiver fitted with an external loopback plug, and back to the ASIC for the selected ports. The port passes the test if the test frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.

- **Node-to-Node (online)** — the Node-to-Node test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes the test if the frame that was sent by the ASIC matches the frame that was received. This test does not disrupt communication on the selected port. This test requires that the port be online, and therefore, does not disrupt communication.

To run the internal, external, or online port loopback test on a port, perform the following procedure:

1. Select the port to be tested in the faceplate display.
2. Select **Port > Port Loopback Test** to open the Port Loopback Test dialog.
3. Select **Internal**, **External**, or **Online** in the Test Selection area.
4. Click **OK** and McDATA Web Server will change the port state. If you choose **Internal** or **External**, McDATA Web Server will prompt you to confirm that the port state needs to be changed to the diagnostic state. If you selected **External**, verify a loopback plug has been installed.
5. Enter the frame count, frame size, and select a test pattern option. You may use the default pattern or enter an 8-digit pattern (hex). Select **Terminate Test Upon Error** for online test, if you want the test to stop should it encounter an error.
6. Click **Start Test** to begin the test. The Test Results area displays the test status, number of frames sent, and number of errors found.
7. To test another port, open the **Select Port** drop-down list and select another port (number) and test type (**Internal**, **External**, or **Online**) in the Test Selection area.
8. Click **Start Test** to begin the next test. Observe the results in the Test Results area.

5 Command Line Interface

The Command Line Interface (CLI) enables you to perform a variety of fabric and switch management tasks through an Ethernet connection. This section describes the following:

- [Logging on to a 4Gb SAN Switch](#), page 105
- [User accounts](#), page 105
- [Working with switch configurations](#), page 106
- [Commands](#), page 108

Logging on to a 4Gb SAN Switch

To log on to a switch using Telnet, open a command line window on the workstation and enter the Telnet command followed by the switch IP address:

```
# telnet ip_address
```

A Telnet window opens prompting you for a login. Enter an account name and password.


User accounts

The McDATA 4Gb SAN Switch comes from the factory with the following user account already defined:

```
Account name: admin  
Password: password  
Authority: Admin
```

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account.

- Refer to "[Commands](#)" on page 108 for information about authority levels.
- Refer to the "[User command](#)" on page 203 for information about creating user accounts.
- Refer to "[Passwd command](#)" on page 140 for information about changing passwords.

 **NOTE:** A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
 - 9 high priority Telnet sessions
 - 6 McDATA Web Server and/or Telnet logins. Additional logins will be refused.
 - If the entry switch has SSL (Secure Socket Layer) enabled, the switch will generate and display a Verify Certificate dialog that you must accept before gaining access to the fabric. Refer to "[Connection security](#)" on page 30 and "[System Services dialog](#)" on page 80 for more information on certificates and SSL.
-

Working with switch configurations

Successful management of switches and fabrics with the CLI depends on the effective use of switch configurations. Modifying configurations, backing up configurations, and restoring configurations are key switch management tasks.

Modifying a configuration

A switch supports up to 10 configurations including the default configuration. Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components. The Show Switch command displays the name of the active configuration. A configuration name can have up to 31 characters excluding the pound symbol (#), semicolon (;), and comma (,). By editing the latest configuration and saving the results under a new name, you can create a history of configuration changes. Use the Config List command to display the configurations stored on the switch.

```
McDATA4GbSAN #> config list
Current list of configurations
-----
default
config_10132003
```

To modify a switch configuration you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or McDATA Web Server. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed. The Config Edit session provides access to the Set Config commands with which you make modifications to the port, switch, port threshold alarm, or zoning configuration components as shown:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit default
The config named default is being edited.
McDATA4GbSAN (admin-config)#> set config port . . .
McDATA4GbSAN (admin-config)#> set config switch . . .
McDATA4GbSAN (admin-config)#> set config threshold . . .
McDATA4GbSAN (admin-config)#> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named Default are being saved to a new configuration named config_10132003. However, the new configuration does not take effect until you activate it with the Config Activate command:

```
McDATA4GbSAN (admin-config)#> config save config_10132003
McDATA4GbSAN (admin)#> config activate config_10132003
McDATA4GbSAN (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

Backing up and restoring switch configurations

Backing up and restoring a configuration is useful to protect your work or for use as a template in configuring other switches. The Config Backup command creates a file on the switch, named `configdata`. This file can be used to restore a switch configuration only from the CLI; it cannot be used to restore a switch using McDATA Web Server.

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config backup
```

The `configdata` file contains all of the switch configuration information including the following:

- All named switch configurations including the default configuration. This includes port, switch, port threshold alarm, and zoning configuration components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database included all zone sets, zones, and aliases

You use FTP to download the `configdata` file to your workstation for safe keeping and to upload the file back to the switch for the restore function. To download the `configdata` file, open an FTP session on the switch and log in with the account name “images” and password “images”. Transfer the file in binary mode with the Get command as shown:

```
>ftp ip_address
user:images
password: images
ftp>bin
ftp>get configdata
xxxxx bytes sent in xx secs.
ftp>quit
```

You should rename the `configdata` file on your workstation with the switch name and date, `config_switch_169_10112003`, for example.

The restore operation begins with FTP to upload the configuration file from the workstation to the switch, then finishes with a Telnet session and the Config Restore command. To upload the configuration file, `config_switch_169_10112003` in this case, open an FTP session with account name “images” and password “images”. Transfer the file in binary mode with the Put command as shown:

```
ftp ip_address
user:images
password: images
ftp> bin
ftp> put config_switch_169_10112003 configdata
Local file config_switch_169_10112003
Remote file configdata
ftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. All management sessions are lost because the switch is reset. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the “[Show Setup command](#)” on page 196. To restore the switch, open a Telnet session, then enter the Config Restore command from within an Admin session as shown:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config restore
The switch will be reset after restoring the configuration.
Please confirm (y/n): [n] y
Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is being
restored - this could take several minutes !]
Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be reset in
3 seconds due to a config restore]
McDATA4GbSAN (admin) #>
Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being reset]
Good bye.
```

Commands

The command syntax is as follows:

```
command  
  operand  
  operand [value]  
  operand [value1] [value2]
```

The command is followed by one or more operands. Consider the following rules and conventions:

- Commands and operand are case insensitive.
- Required operand values appear in standard font: [value]. Optional values are shown in italics: [value].
- Underlined portions of the operand in the command format indicate the abbreviated form that can be used. For example the Delete operand can be abbreviated Del.

The command-line completion feature makes entering and repeating commands easier. [Table 27](#) describes the command-line completion keystrokes.

Table 27 Command line completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press Tab to complete the command line. Press Tab again to display all possibilities if more than one possibility exists.
Up Arrow	Scrolls backward through the list of previously entered commands
Down Arrow	Scrolls forward through the list of previously entered commands
Control+A	Moves the cursor to the beginning of the command line
Control+E	Moves the cursor to the end of the command line

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an Admin session. An account must have Admin authority to enter the Admin Start command, which opens an Admin session. Refer to the "[Admin command](#)" on page 110. The commands and their page numbers are listed in [Table 28](#).

Table 28 Commands listed by authority level

Monitoring commands		Configuration command	
Help	(133)	Admin	(110)
History	(134)	Admin session commands	
Ping	(141)	Alias ¹	(111)
Ps	(142)	CIM ¹	(113)
Quit	(143)	CIMListener	(114)
Show	(178)	CIMSubscription	(116)
Show Config	(188)	Config ¹	(118)
Show Log	(191)	Create	(121)
Show Perf	(194)	Date ¹	(124)
Show Setup	(196)	Feature	(125)
Uptime	(202)	Firmware Install	(126)
Whoami	(205)	Group ¹	(127)
		Hardreset	(132)
		Hotreset	(135)
		Image	(136)
		Lip	(139)
		Passwd	(140)
		Reset	(144)
		Security	(149)
		Securityset ¹	(152)
		Set ¹	(154)
		Set Config	(156)
		Set Log	(166)
		Set Port ¹	(169)
		Set Setup	(170)
		Shutdown	(199)
		Test	(200)
		User ¹ 2	(203)
		Zone ¹	(206)
		Zoneset ¹	(209)
		Zoning ¹	(211)

1. Some operands do not require an Admin session.

2. Some operands can be executed only by the Admin account name.

Admin command

Description Starts and ends an Admin session. The Admin session allows commands that change the fabric and switch configurations. Only one Admin session can be started on the switch at any time. An idle Admin session will time out after a period of time (the default is 30 minutes) which can be changed using the Set Setup System command.

Authority Admin

Syntax admin
start (or begin)
end (or stop)
cancel

Operands start or begin
Opens the Admin session.

end (or stop)
Terminates the Admin session. The Hardreset, Hotreset, Logout, Shutdown, and Reset Switch commands will also end an Admin session. A a Set Setup System command will also end an Admin session if the IP address changed.

cancel
Terminates an Admin session opened by another user. Use this operand with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an Admin session does not release the session. In this case, you must either wait for the Admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
McDATA4GbSAN #> admin start

McDATA4GbSAN (admin) #>

.
.
.

McDATA4GbSAN (admin) #> admin end
McDATA4GbSAN #>
```

See also [Set Setup command](#), page 170

Alias command

Description Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session for all operands except List and Members

Syntax alias
add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Operands add [alias] [member_list]

Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). The domain ID in Standard interop mode (default) should be unique and within the 97–127 range. This is equivalent to 1–31 when in McDATA Fabric interop mode. Port numbers can be 0–255.
- 16-character hexadecimal world wide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]

Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]

Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, \$, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]

Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all aliases. This operand does not require an Admin session.

members [alias]

Displays all members of the alias given by [alias]. This operand does not require an Admin session.

remove [alias] [member_list]

Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 97–127; port numbers can be 0–255.
- 16-character hexadecimal world wide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

```
rename [alias_old] [alias_new]
```

Renames the alias given by [alias_old] to the alias given by [alias_new].

CIM command

Description Manages CIM listener and subscription configurations on the switch.

Authority Admin session

Syntax cim
cancel
clear
edit
limits
save

Operands cancel
Terminates the current CIM edit session without saving changes that were made.

clear
Clears all CIM listener and subscription configurations from the switch.

edit
Opens a CIM edit session.

limits
Displays the maximum allowed number of CIM listeners, subscriptions, and subscriptions per listener. This operand does not require an Admin session nor a CIM edit session.

save
Saves all changes made during the current CIM edit session.

Examples The following is an example of the CIM Edit command:

```
McDATA4GbSAN (admin) #> cim edit
McDATA4GbSAN (admin-cim) #> cimlistener create CIM_listener_1
.
.
.
```

```
McDATA4GbSAN (admin-cim) #> cim save
```

The following is an example of the CIM Limits command:

```
McDATA4GbSAN #> cim limits
```

Cim Attribute	Maximum
-----	-----
MaxListeners	32
MaxSubscriptions	50
MaxSubscriptionsPerListener	6

See also [CIMListener command](#), page 114
[CIMSubscription command](#), page 116

CIMListener command

Description Configures CIM indication service listeners and adds subscriptions to listeners. Refer to the CIMSubscription command for information about configuring subscriptions.

Authority Admin session and a CIM Edit session. Refer to the CIM command for information about opening a CIM edit session.

Syntax cimlistener
add [listener_name] [subscription_list]
create [listener_name]
delete [listener_name]
edit [listener_name]

Operands add [listener_name] [subscription_list]
Adds the set of subscriptions given by [subscription_list] to the listener given by [listener_name]. Use a <space> to delimit subscription names in [subscription_list].

create [listener_name]
Prompts you in a line-by-line fashion to create a CIM listener with the name given by [listener_name]. [listener_name] can have up to 32 characters: 0–9, A–Z, a–z, _, \$, ^, and -. The CIM listener configuration parameters are described in [Table 29](#).

Table 29 CIM listener configuration parameters

Parameter	Description
Name	Listener name
Type	Listener type: <ul style="list-style-type: none">• Permanent — send indications to the CIM client whether a connection can be established or not. This is the default.• Transient — sends indications to the CIM client, but ceases if a connection cannot be established after 60 minutes.
URL	IP address of the CIM client and the port number to which to send indications. The default is 10.0.0.1:5000.

delete [listener_name]
Deletes the listener given by [listener_name] from the CIM database.

edit [listener_name]
Opens an editing session in which you can modify the CIM listener given by [listener_name]. Refer to [Table 29](#) for a description of the CIM listener configuration parameters.

Examples The following is an example of the CIMListener Create command:

```
McDATA4GbSAN (admin-cim) #> cimlistener create listener_1
```

```
A list of attributes with formatting and current values will follow.  
Enter a new value or simply press the ENTER key to accept current value.  
If you wish to terminate this process before reaching the end of the list  
press 'q' or 'Q' and the ENTER key to do so.
```

```
Name listener_1  
Type (2=Permanent, 3=Transient) [Permanent ]  
URL (IP address:port format) [10.0.0.1:5000]
```

```
Finished configuring attributes.  
This configuration must be saved with the cim save command  
before it can take effect, or to discard this configuration  
use the cim cancel command.
```

See also [CIM command](#), page 113

[CIMSubscription command](#), page 116

CIMSubscription command

Description Creates, edits, or removes CIM subscriptions.

Authority Admin session and a CIM Edit session.

Syntax `cimsubscription`
`create [subscription_name]`
`delete [subscription_name]`
`edit [subscription_name]`

Operands `create [subscription_name]`
Prompts you in a line-by-line fashion to create a CIM subscription with the name given by `[subscription_name]`. `[subscription_name]` can have up to 32 characters: 0–9, A–Z, a–z, _, \$, ^, and -. [Table 30](#) describes the CIM subscription configuration parameters.

Table 30 CIM Subscription configuration parameters

Parameter	Description
Name	Subscription name
FilterID	Event type for which the switch monitors and sends an indication to the CIM client. The event types are as follows: CreateComputerSystem — a switch is added to the fabric. This is the default. ModifyComputerSystem — a switch state change DeleteComputerSystem — a switch is removed from the fabric CreateFCPort — not supported ModifyFCPort — an FC port state change DeleteFCPort — not supported
EnabledState	Enable (True) or disable (False) the subscription. The default is True.
Duration	Subscription life span in seconds. The subscription life span begins when the subscription is created. Expired subscriptions do not send indications to the CIM client though they remain in the CIM database. Values can be 1–720000. 0 indicates indefinite, which is the default.

`delete [subscription_name]`
Deletes the subscription given by `[subscription_name]` from the CIM database.

`edit [subscription_name]`
Opens an editing session in which you can modify the CIM subscription given by `[subscription_name]`. Refer to [Table 30](#) for a description of the CIM subscription configuration parameters.

Examples The following is an example of the CIMSubscription Create command:

```
McDATA4GbSAN (admin-cim) #> cimsubscription create subscription_1
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value. If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.

```
FilterID values:  1 = Create:ComputerSystem
                  2 = Modify:ComputerSystem
                  3 = Delete:ComputerSystem
                  4 = Create:FCPort
                  5 = Modify:FCPort
                  6 = Delete:FCPort
```

```
Name           subscription_1
FilterID       (see allowed options above)      [Create:ComputerSystem]
EnabledState   (True / False)                  [True                ]
Duration      (decimal value, 0-720000 secs, 0=forever) [0                    ]
```

Finished configuring attributes.
This configuration must be saved with the cim save command before it can take effect, or to discard this configuration use the cim cancel command.

See also [CIM command](#), page 113

[CIMListener command](#), page 114

Config command

Description Manages the FC configurations on a switch. For information about setting the port and switch configurations, refer to the Set Config command.

Authority Admin session for all operands except List.

Syntax `config`
`activate [config_name]`
`backup`
`cancel`
`copy [config_source] [config_destination]`
`delete [config_name]`
`edit [config_name]`
`list`
`restore`
`save [config_name]`

Operands `activate [config_name]`

Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

`backup`

Creates a file named `configdata`, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of "images" for both, and enter "get configdata". Refer to "[Backing up and restoring switch configurations](#)" on page 107.

`cancel`

Terminates the current configuration edit session without saving changes that were made.

`copy [config_source] [config_destination]`

Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

`delete [config_name]`

Deletes the configuration given by [config_name] from the switch. You cannot delete the default configuration (Default Config) nor the active configuration.

`edit [config_name]`


Begins an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.


`list`

Displays a list of all available configurations on the switch. This operand does not require an Admin session.

restore

Restores configuration settings to an out-of-band switch from a backup file named `configdata`, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command. After the restore is complete, the switch automatically resets. Refer to "[Backing up and restoring switch configurations](#)" on page 107.

 **NOTE:** All management sessions are terminated because the switch is reset. Use the Set Setup System command to return the IP configuration to the values you want.

 **NOTE:** Configuration archive files created with the McDATA Web Server Archive function are not compatible with the Config Restore command.

save *[config_name]*

Saves changes made during a configuration edit session in the configuration given by `[config_name]`. If you omit `[config_name]`, the value for `[config_name]` you chose for the most recent Config Edit command is used. `[config_name]` can be up to 31 characters excluding #, semicolon (;), and comma (,). The switch supports up to 10 configurations including the default configuration.

Notes If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples The following shows an example of how to open and close a Config Edit session:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit
    The config named default is being edited.
.
.
McDATA4GbSAN (admin-config) #> config cancel
    Configuration mode will be canceled. Please confirm (y/n): [n] y
McDATA4GbSAN (admin) #> admin end
```

The following is an example of how to create a backup file (`configdata`) and download the file to the workstation.

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config backup
McDATA4GbSAN (admin) #> admin end
McDATA4GbSAN #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```

The following is an example of how to upload a configuration backup file (`configdata`) from the workstation to the switch, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config restore
The switch will be reset after restoring the configuration.
Please confirm (y/n): [n] y
Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is
being restored - this could take several minutes !]
Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be
reset in 3 seconds due to a config restore]
McDATA4GbSAN (admin) #>
Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being
reset]
Good bye.
```

See also [Set Setup command](#), page 170.

Create command


Description Creates support files for troubleshooting switch problems, and certificates for secure communications for McDATA Web Server.

Authority Admin session

Syntax create
 certificate
 support

Operands certificate

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as McDATA Web Server. The certificate is valid 24 hours before the certificate creation date (due to potential switch/workstation time differences) and expires 365 days after the creation date. Should the current certificate become invalid, use the Create Certificate command to create a new one.

 **NOTE:** To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. Refer to the following:

- Date command for information about setting the time and date
 - Set command (Timezone operand) for information about setting the time zone on the switch and workstation
 - Set Setup command (System operand) for information about enabling the Network Time Protocol for synchronizing the time and date on the switch and workstation from an NTP server.
-

support

Assembles all log files and switch memory data into a archive file (`dump_support.tgz`) on the switch. If your workstation has an FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation. The support file is useful to technical support personnel for troubleshooting switch problems. Use this command when directed by your authorized maintenance provider.

Examples The following is an example of the Create Support command when an FTP server is available on the workstation:

```
McDATA4GbSAN (admin) #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): y
Enter IP Address of remote computer: 10.20.33.130
Login name: johndoe
Enter remote directory name: bin/support
Would you like to continue downloading support file? (y/n) [n]: y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxx

230 User johndoe logged in.
cd bin/support
250 CWD command successful.
lcd /itasca/conf/images
Local directory now /itasca/conf/images
bin
200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

The following is an example of the Create Support command and how to download the support file to your workstation. When prompted to send the support file to another machine, decline, then close the Telnet session. Open an FTP session on the switch and log in with the account name "images" and password "images". Transfer the `dump_support.tgz` file in binary mode with the Get command.

```
McDATA4GbSAN (admin) #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n

McDATA4GbSAN (admin) #> quit
>ftp switch_ip_address
user: images
password: images

ftp>bin
ftp>get dump_support.tgz
xxxxx bytes sent in xx secs.
ftp>quit
```

The following is an example of the Create Certificate command:

```
McDATA4GbSAN (admin) #> create certificate
The current date and time is day mon date hh:mm:ss UTC yyyy.
This is the time used to stamp onto the certificate.
Is the date and time correct? (y/n): [n] y
Certificate generation successful.
```

See also [Date command](#), page 124
[Set command](#), page 154
[Set Setup command](#), page 170

Date command

Description This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax `date`
`[MMDDhhmmCCYY]`

Operands `[MMDDhhmmCCYY]`
Specifies the date – this requires an Admin session. If you omit `[MMDDhhmmCCYY]`, the current date is displayed which does not require an Admin session.

Notes Network Time Protocol (NTP) must be disabled to set the time with the Date command. Refer to the Set Setup command, System operand, for information about NTP.

When setting the date and time on a switch that is enabled for SSL connections, the switch time must be within 24 hours of the workstation time. Otherwise, the connection will fail.

Examples The following is an example of the Date command:

```
McDATA4GbSAN #> date
Mon Apr 07 07:51:24 2005
```

See also [Date command](#), page 124

[Set command](#), page 154

Feature command

Description Adds Product Feature Enablement (PFE) key features to the switch and displays the PFE key log. A Product Feature Enablement (PFE) key is a password that you can purchase from your switch distributor or authorized reseller to enable particular features in your switch. The SANtegrity Enhanced PFE key enables device security on the switch.

To obtain the McDATA 4Gb SAN Switch serial number and Product Feature Enablement license key, follow the step-by-step instructions on the "firmware feature entitlement request certificate" for the PFE key. One of the license key retrieval options is via the web: www.webkey.external.hp.com.

Authority Admin session for Add operand only

Syntax feature
 add [pfe_key]
 log

Operands add [pfe_key]
 Adds the feature that corresponds to the value given by [pfe_key]. [pfe_key] is case insensitive.

log
 Displays a list of installed PFE key features.

Notes If the PFE key instructions indicate that the procedure is disruptive, isolate the switch from the fabric before installing the PFE key.

Firmware Install command

Description Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch (without a POST) to activate the firmware. This command is disruptive, and prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

Authority Admin session

Syntax `firmware install`

Examples The following is an example of the Firmware Install command:

```
McDATA4GbSAN (admin) #> firmware install
Warning: Installing new firmware requires a switch reset. Continuing with
this action will terminate all management sessions, including any Telnet
sessions. When the firmware activation is complete, you may log in to the
switch again.


Do you want to continue? [y/n]: y
Press 'q' and the ENTER key to abort this command.

User Account : johndoe
IP Address : 10.20.20.200
Source Filename : 5.2.x.xx.xx_mpc

About to install image. Do you want to continue? [y/n] y
Connected to 10.20.20.200 (10.20.20.200).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password:*****
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Group command

Description Creates groups, manages membership within the group, and manages the membership of groups in security sets.

 **IMPORTANT:** This command is available only with the SANtegrity Enhanced PFE key.

Authority Admin session and a Security Edit session. Refer to the Security command for information about starting a Security Edit session. The List, Members, Securitysets, and Type operands are available without an Admin session.

Syntax

```
group
  add [group]
  copy
  create [group] [type]
  delete [group]
  edit [group] [member]
  list
  members [group]
  remove [group] [member_list]
  rename [group_old] [group_new]
  securitysets [group]
  type [group]
```

Operands Edit
Initiates an editing session in which to specify a group member and its attributes for the existing group given by [group]. ISL, Port, and MS member attributes are described in [Table 31](#), [Table 32](#), and [Table 33](#) respectively. The group name and group type attributes are read-only fields common to all three tables.

Table 31 ISL Group member attributes

Attribute	Description
Member	World Wide Name of the switch that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using Challenge Handshake Authentication Protocol. The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the ISL member. The hash functions are MD5 or SHA-1. If the ISL member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the ISL group member. The string has the following lengths depending on the Primary Hash function: <ul style="list-style-type: none">• MD5 hash: 16-byte• SHA-1 hash: 20-byte

Table 31 ISL Group member attributes (continued)

Attribute	Description
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the ISL group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the ISL group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: <ul style="list-style-type: none"> • MD5 hash: 16-byte • SHA-1 hash: 20-byte

Table 32 Port Group member attributes

Attribute	Description
Member	Port World Wide Name for the N_Port device that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using Challenge Handshake Authentication Protocol. The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the Port group member. The hash functions are MD5 or SHA-1. If the Port group member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the Port group member. The string has the following lengths depending on the Primary Hash function: MD5 hash: 16-byte SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the Port group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the Port group member. The Primary Hash and the Secondary Hash cannot be the same.

Table 33 MS Group member attributes

Attribute	Description
Member	Port World Wide Name for the N_Port device that would attach to the switch
CTAuthentication	Common Transport (CT) authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Hash	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Secret	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: MD5 hash: 16-byte SHA-1 hash: 20-byte

`copy [group_source] [group_destination]`

Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

`create [group] [type]`

Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, \$, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. [type] can be one of the following:

ISL

Configures security for attachments to other switches.

Port

Configures security for attachments to N_Port devices.

MS

Configures security for attachments to N_Port devices that are issuing management server commands.

`edit [group] [member]`

Initiates an editing session in which to change the attributes of a World Wide Name given by [member] in a group given by [group]. Member attributes that can be changed are described in [Table 34](#):

Table 34 Group member attributes

Attribute	Description
Authentication (ISL and Port Groups)	Enables (CHAP) or disables (None) authentication using Challenge Handshake Authentication Protocol. The default is None.
CTAuthentication (MS Groups)	CT authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Primary Hash (ISL and Port Groups)	The preferred hash function to use to decipher the encrypted Primary Secret sent by the member. The hash functions are MD5 or SHA-1. If the member does not support the Primary Hash, the switch will use the Secondary Hash.
Hash (MS Groups)	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Primary Secret (ISL and Port Groups)	Hexadecimal string that is encrypted by the Primary Hash for authentication with the member. The string has the following lengths depending on the Primary Hash function: MD5 hash: 16-byte SHA-1 hash: 20-byte
Secondary Hash (ISL and Port Groups)	Hash function to use to decipher the encrypted Secondary Secret sent by the group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret (ISL and Port Groups)	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: MD5 hash: 16-byte SHA-1 hash: 20-byte

Table 34 Group member attributes (continued)

Attribute	Description
Secret (MS Groups)	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: MD5 hash: 16-byte SHA-1 hash: 20-byte
Binding (ISL Groups)	Domain ID of the switch to which to bind the ISL group member World Wide Name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. 0 (zero) specifies no binding.

list

Displays a list of all groups and the security sets of which they are members. This operand is available without an Admin session.

members [group]

Displays all members of the group given by [group]. This operand is available without an Admin session.

remove [group] [member_list]

Remove the port/device World Wide Name given by [member] from the group given by [group]. Use a <space> to delimit multiple member names in [member_list]

rename [group_old] [group_new]

Renames the group given by [group_old] to the group given by [group_new].

securitysets [group]

Displays the list of security sets of which the group given by [group] is a member. This operand is available without an Admin session.

type [group]

Displays the group type for the group given by [group]. This operand is available without an Admin session.

Examples The following is an example of the Group Add command:

```
McDATA4GbSAN (admin-security) #> group add Group_1
A list of attributes with formatting and default values will follow
Enter a new value or simply press the ENTER key to accept the current value
with exception of the Group Member WWN field which is mandatory.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
Group Name          Group_1
Group Type          ISL
Member              (WWN)                [00:00:00:00:00:00:00:00]
Authentication      (None / Chap)          [None]
PrimaryHash         (MD5 / SHA-1)          [MD5]
PrimarySecret       (32 hex or 16 ASCII char value) [
SecondaryHash       (MD5 / SHA-1 / None)    [None]
SecondarySecret     (40 hex or 20 ASCII char value) [
Binding             (domain ID 97-127, 0=None) [0]

Finished configuring attributes.
To discard this configuration use the security cancel command.
```

The following is an example of the Group Edit command:

```
McDATA4GbSAN (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end of
the list press 'q' or 'Q' and the ENTER key to do so.
Group Name          g1
Group Type          ISL
Group Member        10:00:00:c0:dd:00:90:a3
Authentication      (None / Chap)          [None]  chap
PrimaryHash         (MD5 / SHA-1)          [MD5 ]  sha-1
PrimarySecret       (40 hex or 20 ASCII char value) [   ]  1234567890123456789
SecondaryHash       (MD5 / SHA-1 / None)      [None]  md5
SecondarySecret     (32 hex or 16 ASCII char value) [   ]  1234567890123456
Binding             (domain ID 97-127, 0=None) [3   ]
```

Finished configuring attributes.
To discard this configuration use the security cancel command.

The following is an example of the Group List command:

```
McDATA4GbSAN #> group list
Group          SecuritySet
-----
group1 (ISL)
              alpha
group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
McDATA4GbSAN #> group members group1
Current list of members for Group: group1
-----
10:00:00:c0:dd:00:71:ed
10:00:00:c0:dd:00:72:45
10:00:00:c0:dd:00:90:ef
10:00:00:c0:dd:00:b8:b7
```

See also [Security command](#), page 149
[Securityset command](#), page 152
[Set Config command](#), page 156.

Hardreset command

Description Resets the switch and performs a POST. This reset disrupts traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, refer to the Set Log command.

Authority Admin session

Syntax `hardreset`

Notes To reset the switch without a POST, refer to the Reset command.

To reset the switch without disrupting traffic, refer to the Hotreset command.

See also [Hotreset command](#), page 135

[Reset command](#), page 144

[Set Log command](#), page 166

Help command

Description Displays a brief description of the specified command, its operands, and usage.

Authority None

Syntax `help [command] [operand]`

Operands [command]

Displays a summary of the command given by [command] and its operands. If you omit [command], the system displays all available commands.

[operand]

Displays a summary of the operand given by [operand] belonging to the command given by [command]. If you omit [operand], the system displays the available operands for the specified command.

all

Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Config command:

```
McDATA4GbSAN #> help config
config CONFIG_OPTIONS
The config command operates on configurations.
```

```
Usage: config { activate | backup | cancel | copy | delete |
               edit | list | restore | save }
```

The following is an example of the Help Config Edit command:

```
McDATA4GbSAN #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created. If it is not given, the currently active configuration is edited.
```

Admin mode is required for this command.

```
Usage: config edit [CONFIG_NAME]
```

History command

Description Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax history

Notes Use the History command to provide context for the ! command:

- Enter ![command_string] to re-execute the most recent command that matches [command_string].
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
McDATA4GbSAN #> history
```

```
 1 show switch
 2 date
 3 help set
 4 history
```

```
McDATA4GbSAN #> !3
```

```
help set
```

```
set SET_OPTIONS
```

```
There are many attributes that can be set.
```

```
Type help with one of the following to get more information:
```

```
Usage: set { alarm | beacon | config | log | pagebreak |
            port | setup | switch }
```

Hotreset command

Description Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the event log. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds. To save the event log to a file before resetting, refer to the Set Log command.

Authority Admin session

Syntax hotreset

Notes You can load and activate firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices under the following conditions:

- The current firmware version is a version that supports upgrading to the new version
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes
- No port in the fabric is in the diagnostic state
- No zoning changes are being made in the fabric
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, McDATA Web Server sessions reconnect automatically. However, Telnet sessions must be restarted manually.

This command clears the event log and all counters.

See also [Hotreset command](#), page 135

Image command

Description Manages and installs switch firmware.

Authority Admin session

Syntax image
cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
install
list
unpack [file]

Operands cleanup
Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]
Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the FTP server with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the FTP server, the system will prompt you for it.

install
Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch (without a POST) to activate the firmware. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

list
Displays the list of image files that reside on the switch.

unpack [file]
Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

To install firmware when the management workstation has an FTP server, use the Image Install command or the Firmware Install command. To install firmware when the management workstation does not have an FTP server, perform the following procedure:

1. Connect to the switch through the Ethernet port.
2. Move to the folder or directory on the workstation that contains the new firmware image file.
3. Establish communications with the switch using the File Transfer Protocol (FTP). Enter the following on the command line:

```
>ftp xxx.xxx.xxx.xxx
```

where xxx.xxx.xxx.xxx is the switch IP address is the switch name associated with the IP address.

4. Enter the following account name and password:
user:images
password: images
5. Activate binary mode and copy the firmware image file on the switch:

```
ftp>bin  
ftp>put filename
```

6. Wait for the transfer to complete, then close the FTP session.

```
xxxxx bytes sent in xx secs.  
ftp>quit
```

7. Establish communications with the switch using the CLI. Enter the following on the command line:

```
telnet xxx.xxx.xxx.xxx
```

where xxx.xxx.xxx.xxx is the switch IP address is the switch name associated with the IP address.

8. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name is "admin", and password is "password".
9. Open an Admin session to acquire the necessary authority.

```
McDATA4GbSAN $>admin start
```

10. Display the list of firmware image files on the switch to confirm that the file was loaded.

```
McDATA4GbSAN (admin) $>image list
```

11. Unpack the firmware image file to install the new firmware in flash memory.

```
McDATA4GbSAN (admin) $>image unpack filename
```

12. Wait for the unpack to complete.

```
image unpack command result: Passed
```

13. A message will prompt you to reset the switch to activate the firmware. Resetting the switch is disruptive. Use the Hotreset command to attempt a non-disruptive activation.

```
McDATA4GbSAN (admin) $>hotreset
```

Examples The following is an example of the Image Install command:

```
McDATA4GbSAN (admin) #> image install
Warning: Installing new firmware requires a switch reset.
Continuing with this action will terminate all management sessions,
including any Telnet sessions. When the firmware activation is complete,
you may log in to the switch again.
Do you want to continue? [y/n]: y
    Press 'q' and the ENTER key to abort this command.

User Account      : johndoe
IP Address        : 10.20.33.130
Source Filename   : 5.2.00.11_mpc

About to install image. Do you want to continue? [y/n] y

Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
    This may take several seconds...
    The switch will now reset.
Connection closed by foreign host.
```

See also [Firmware Install command](#), page 126

Lip command

Description Re-initializes the specified loop port.

Authority Admin session

Syntax lip [port_number]

Operands [port_number]
The number of the port to be re-initialized.

Examples The following is an example of the Lip command:

```
McDATA4GbSAN (admin) #> lip 2
```

Passwd command

Description Changes a user account's password.

Authority Admin account name and an Admin session to change another account's password. You can change you own password without an Admin session.

Syntax `passwd [account_name]`

Operands `[account_name]`

The user account name. To change the password for an account name other than your own, you must open an Admin session with the account name Admin. If you omit `[account_name]`, you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
McDATA4GbSAN (admin) #> passwd user2
```

```
Press 'q' and the ENTER key to abort this command.
```

```
account OLD password : *****
account NEW password (8-20 chars) : *****
```

```
please confirm account NEW password: *****
password has been changed.
```

See also [User command](#), page 203

Ping command

Description Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax ping [ip_address]

Operands [ip_address]

The IP address of the switch to query. Broadcast IP addresses, such as 255.255.255.255, are not valid.

Examples The following is an example of a successful Ping command:

```
McDATA4GbSAN #> ping 10.20.11.57
Ping command issued. Waiting for response...
McDATA4GbSAN #>
Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
McDATA4GbSAN #> ping 10.20.10.100
Ping command issued. Waiting for response...
No response from 10.20.10.100. Unreachable.
```

Ps command

Description Displays current system process information.

Authority None

Syntax ps

Examples The following is an example of the Ps command:

```
McDATA4GbSAN #> ps
```

PID	PPID	%CPU	TIME	ELAPSED	COMMAND
338	327	0.0	00:00:00	3-01:18:35	cns
339	327	0.0	00:00:01	3-01:18:35	ens
340	327	0.0	00:00:21	3-01:18:35	dlog
341	327	0.1	00:05:35	3-01:18:35	ds
342	327	0.2	00:11:29	3-01:18:35	mgmtApp
343	327	0.0	00:00:04	3-01:18:35	fc2
344	327	0.0	00:02:16	3-01:18:35	nserver
345	327	0.0	00:02:44	3-01:18:35	mserver
346	327	0.8	00:35:12	3-01:18:35	util
347	327	0.0	00:00:29	3-01:18:35	snmpservicepath
348	327	0.0	00:02:46	3-01:18:34	eport
349	327	0.0	00:00:21	3-01:18:34	PortApp
350	327	5.6	04:08:24	3-01:18:34	port_mon
351	327	0.0	00:01:38	3-01:18:34	zoning
352	327	0.0	00:00:01	3-01:18:34	diagApp
404	327	0.0	00:00:04	3-01:18:27	snmpd
405	327	0.0	00:00:02	3-01:18:27	snmpmain
406	405	0.0	00:00:00	3-01:18:26	snmpmain

Quit command

Description Closes the Telnet session.

Authority None

Syntax quit, exit, or logout

Notes You can also press **Control+D** to close the Telnet session.

Reset command

Description Resets the switch configuration parameters. If you omit the operand, the default is Reset Switch.

Authority Admin session

Syntax reset
 cim
 config [*config_name*]
 factory
 port [*port_number*]
 radius
 security
 services
 snmp
 switch (default)
 system
 zoning

Operands cim

Resets cim configuration to default values.

config [*config_name*]

Resets the configuration given by [*config_name*] to the factory default values for switch, port, port threshold alarm, and zoning configuration as described in [Table 35](#) through [Table 38](#). If [*config_name*] does not exist on the switch, a configuration with that name will be created. If you omit [*config_name*], the active configuration is reset. You must activate the configuration for the changes to take effect. for switch, port, and port threshold alarm configuration default values.

factory

Resets switch configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, security configuration, RADIUS configuration, switch services configuration, and zoning to the factory default values as described in [Table 35](#) through [Table 43](#). The switch configuration is activated automatically.

port [*port_number*]

Re-initializes the port given by [*port_number*]. External ports are numbered 0 and 9; internal ports are numbered 1–8.

radius

Resets the RADIUS configuration to the default values as described in [Table 40](#).

security

Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged.

services

Resets the switch services configuration to the default values as described in [Table 41](#).

snmp

Resets the SNMP configuration settings to the factory default values. Refer to [Table 39](#) for SNMP configuration default values.

switch

Resets the switch without a POST. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware
- Closes all management sessions
- Clears the event log. To save the event log before resetting, refer to the Set Log command

To reset the switch with a POST, refer to the Hardreset command. To reset the switch without disrupting traffic, refer to the Hotreset command.

system

Resets the system configuration settings to the factory default values. Refer to [Table 42](#) for system configuration default values.

zoning

Clears the zoning database and deactivates the active zone set. The zoning configuration values (InteropAutosave, DefaultVisibility, DefaultZone, DiscardInactive) remain unchanged.

Notes The following tables specify the various factory default settings.

Enter the Show Config Switch command to display switch configuration values.

Table 35 Switch configuration defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
DefaultDomain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	McDATA4GbSAN
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	Default Config
InteropMode	Standard

Enter the Show Config Port command to display port configuration values.

Table 36 Port configuration defaults

Parameter	Default
Admin State	Online
Link Speed	Internal ports: 2-Gbps External ports: Auto
Port Type	Internal ports: FL External ports: GL
Symbolic Name	Port <i>n</i> , where <i>n</i> is the port number
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False
ARB_FF	False
InteropCredit	0
FANEnable	True

Table 36 Port configuration defaults (continued)

Parameter	Default
AutoPerfTuning	True
LCFEnable	False
MFSEnable	False
VIEnable	False
MSEnable	True
NoClose	False
PDISCPingEnable	True

Enter Show Config Threshold command to display threshold alarm configuration values.

Table 37 Port threshold alarm configuration defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled	True
RisingTrigger	25
FallingTrigger	1
SampleWindow	10
DecodeErrorsMonitoringEnabled	True
RisingTrigger	200
FallingTrigger	0
SampleWindow	10
ISLMonitoringEnabled	True
RisingTrigger	2
FallingTrigger	0
SampleWindow	10
LoginMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LogoutMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LOSMonitoringEnabled	True
RisingTrigger	100
FallingTrigger	5
SampleWindow	10

Enter the Show Config Zoning command to display zoning configuration values.

Table 38 Zoning configuration defaults

Parameter	Default
InteropAutoSave	True
DefaultVisibility	All
DefaultZone	False
DiscardInactive	True

Enter the Show Setup SNMP command to display SNMP configuration values.

Table 39 SNMP configuration defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<syslocation undefined>
Description	McDATA 4Gb SAN Switch
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.37
AuthFailureTrap	False
ProxyEnabled	True

Enter the Show Setup Radius command to display RADIUS configuration values.

Table 40 RADIUS configuration defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	0
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds
Retries	0
SignPackets	False

Enter the Show Setup Services command to display switch service configuration values.

Table 41 Services configuration defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True
MgmtServerEnabled	False

Enter the Show Setup System command to display system configuration values.

Table 42 System configuration defaults

Parameter	Default
Ethernet Network Discovery	Static
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Admin Timeout	30 minutes
InactivityTimeout	0
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Enter the Show Config Security command to display security configuration values.

Table 43 Security configuration defaults

Parameter	Default
FabricBindingEnabled	True
AutoSave	True


See also [Hardreset command](#), page 132

[Hotreset command](#), page 135

[Set Log command](#), page 166

Security command

Description Opens a Security Edit session in which to manage the security database on a switch. Refer to the Group command and the Securityset command.

 **IMPORTANT:** This command is available only with the SANtegrity Enhanced PFE key.

Authority Admin session. The operands Active, History, Limits, and List are available without an Admin session.

Syntax security
 active
 cancel
 clear
 edit
 history
 limits
 list
 restore
 save

Operands active
 Displays the active security set, its groups, and group members. This operand does not require an Admin session.

cancel
 Ends a Security Edit session without saving changes. Use the Edit operand to open a Security Edit session.

clear
 Clears all inactive security sets from the volatile edit copy of the security database. This operand does not affect the non-volatile security database. However, if you enter the Security Clear command followed by the Security Save command, the non-volatile security database will be cleared from the switch.

edit
 Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To end a Security Edit session and save changes, enter the Security Save command. To end a Security Edit session without saving changes, enter the Security Cancel command.

history
 Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This operand does not require an Admin session.

limits
 Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This operand does not require an Admin session.

list
 Displays all security sets, groups, and group members in the security database. This operand does not require an Admin session.

restore
 Reverts the changes to the security database that have been made during the current Security Edit session since the last Security Save command was entered.

save

Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. Refer to the Securityset command for information about activating a security set.

Examples The following is an example of the Security Active command:

```
McDATA4GbSAN #> security active
Active Security Information

SecuritySet  Group  GroupMember
-----  ----  -----
alpha
                group1 (ISL)
                10:00:00:00:00:10:21:16
                Authentication  Chap
                Primary Hash    MD5
                Primary Secret  *****
                Secondary Hash  SHA-1
                Secondary Secret *****
                Binding          0
                10:00:00:00:00:10:21:17
                Authentication  Chap
                Primary Hash    MD5
                Primary Secret  *****
                Secondary Hash  SHA-1
                Secondary Secret *****
                Binding          0
```

The following is an example of the Security History command:

```
McDATA4GbSAN #> security history
Active Database Information
-----
SecuritySetLastActivated/DeactivatedBy  Remote
SecuritySetLastActivated/DeactivatedOn  day month date time year
Database Checksum                       00000000

Inactive Database Information
-----
ConfigurationLastEditedBy               admin@IB-session11
ConfigurationLastEditedOn               day month date time year
Database Checksum                       00007558
```

The following is an example of the Security Limits command:

```
McDATA4GbSAN #> security limits
Security Attribute  Maximum  Current  [Name]
-----  ----  -
MaxSecuritySets    4        1
MaxGroups          16       2
MaxTotalMembers    1000     19
MaxMembersPerGroup 1000
                4        group1
                15       group2
```

The following is an example of the Security List command:

```
McDATA4GbSAN (admin-security) #> security list
McDATA4GbSAN #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----  -
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----  -
  alpha
      group1 (ISL)
      10:00:00:00:00:10:21:16
      Authentication      Chap
      Primary Hash        MD5
      Primary Secret      *****
      Secondary Hash      SHA-1
      Secondary Secret    *****
      Binding              0
      10:00:00:00:00:10:21:17
      Authentication      Chap
      Primary Hash        MD5
      Primary Secret      *****
      Secondary Hash      SHA-1
      Secondary Secret    *****
      Binding              0
```

See also [Group command](#), page 127
[Securityset command](#), page 152

Securityset command

Description Manages security sets in the security database.



NOTE: This command is available only with the SANtegrity Enhanced PFE key.

Authority Admin session and a Security Edit session. Refer to the Security command for information about starting a Security Edit session. The Active, Groups, and List operands are available without an Admin session. You must end the Security Edit session before using the Activate and Deactivate operands.

Syntax securityset
 activate [security_set]
 active
 add [security_set] [group_list]
 copy [security_set_source] [security_set_destination]
 create [security_set]
 deactivate
 delete [security_set]
 groups [security_set]
 list
 remove [security_set] [group]
 rename [security_set_old] [security_set_new]

Operands activate [security_set]
 Activates the security set given by [security_set]. This operand deactivates the active security set. End the Security Edit session using the Security Save or Security Cancel command before using this operand.

active
 Displays the name of the active security set. This operand is available to without an Admin session.

add [security_set] [group_list]
 Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]
 Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]
 Creates the security set with the name given by [security_set]. A security set name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, \$, ^, and -. The security database supports a maximum of 4 security sets.

deactivate
 Deactivates the active security set. End the Security Edit session before using this operand.

delete [security_set]
 Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]
 Displays all groups that are members of the security set given by [security_set]. This operand is available without an Admin session.

list

Displays a list of all security sets. This operand is available without an Admin session.

remove [security_set] [group]

Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]

Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes Refer to the Group command for information about creating and managing groups.

Examples The following is an example of the Securityset Active command

```
McDATA4GbSAN #> securityset active
Active SecuritySet Information
-----
ActiveSecuritySet alpha
LastActivatedBy Remote
LastActivatedOn day month date time year
```

The following is an example of the Securityset Groups command

```
McDATA4GbSAN #> securityset groups alpha
Current list of Groups for SecuritySet: alpha
-----
group1 (ISL)
group2 (Port)
```

The following is an example of the Securityset List command

```
McDATA4GbSAN #> securityset list
Current list of SecuritySets
-----
alpha
beta
```

See also [Group command](#), page 127

[Security command](#), page 149

Set command

Description Sets a variety of switch parameters.

Authority Admin session for all operands except Alarm, Beacon, and Pagebreak, which are available without an Admin session.

Syntax set
alarm [option]
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]
timezone

Operands alarm [option]
Controls the display of alarms in the session output stream or clears the alarm log. [option] can be one of the following:

clear

Clears the alarm log history. This value requires an Admin session.

on

Enables the display of alarms in the session output stream.

off

Disables the display of alarms in the session output stream.

beacon [state]

Enables or disables the flashing of the Logged-in LEDs according to [state]. This operand does not require an Admin session. [state] can be one of the following:

on

Enables the flashing beacon.

off

Disables the flashing beacon.

config [option]

Sets switch, port, port threshold alarm, security, and zoning configuration parameters. Refer to the Set Config command.

log [option]

Specifies the type of entries to be entered in the event log. Refer to the Set Log command.

pagebreak [state]

Specifies how much information is displayed on the screen at a time according to the value given by [state]. This operand does not require an Admin session. [state] can be one of the following:

on

Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off

Allows continuous display of information without a break.

port [option]

Sets port state and speed for the specified port. The previous Set Config Port settings are restored after a switch reset, port reset, or a reactivation of a switch configuration. Refer to the Set Port command.

setup [option]

Changes SNMP and system configuration settings. Refer to the Set Setup command.

switch [state]

Changes the administrative state for all ports on the switch to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

online

Places all ports online

offline

Places all ports offline.

diagnostics

Prepares all ports for testing.

timezone

Specifies the time zone for the switch and the workstation. The default is Universal Time (UTC) also known as Greenwich Mean Time (GMT). This operand prompts you to choose a region, then a subregion to specify the time zone.

Examples The following examples enables and disables the beacon:

```
McDATA4GbSAN #> set beacon on
```

```
Command succeeded.
```

```
McDATA4GbSAN $> set beacon off
```

```
Command succeeded.
```

See also [Set Config command](#), page 156

[Set Log command](#), page 166

[Set Port command](#), page 169

[Set Setup command](#), page 170

Set Config command

Description Sets switch, port, port threshold alarm, security, and zoning configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command. Refer to the Config command.

Authority Admin session and a Config Edit session

Syntax set config
port [port_number]
ports [port_number]
security
switch
threshold
zoning

Operands port [port_number]
Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. Press **q** to end the configuration for one port, or **qq** to end the configuration for all ports. [Table 44](#) describes the port parameters.

Table 44 Set Config port parameters

Parameter	Description
AdminState	Port administrative state: <ul style="list-style-type: none">• Online — activates and prepares the port to send data. This is the default.• Offline — prevents the port from receiving signal and accepting a device login• Diagnostics — prepares the port for testing and prevents the port from accepting a device login• Down — disables the port by removing power from the port lasers
LinkSpeed	Transmission speed: Internal ports: 2-Gbps External ports: Auto, 1-Gbps, 2-Gbps, 4-Gbps
PortType	Internal ports: FL External ports: GL, G, FL, F
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is Port <i>n</i> , where <i>n</i> is the port number.
ALFairness	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False.

Table 44 Set Config port parameters (continued)

Parameter	Description
ARB_FF	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit (External ports only)	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (8) is unchanged. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
FANEnable	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.
AutoPerfTuning	Automatic performance tuning for FL_Ports only. The default is True. <ul style="list-style-type: none"> If AutoPerfTuning is enabled (True) and the port is an FL_Port, MFSEnable is automatically enabled. LCFEnable and VIEnable are overridden to False. If AutoPerfTuning is disabled (False), MFSEnable, LCFEnable, and VIEnable retain their original values.
LCFEnable	Link control frame preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. This parameter appears only if AutoPerfTuning is False. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is False. Enabling MFSEnable disables LCFEnable and VIEnable.
VIEnable	Virtual Interface (VI) preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.
PDISCPingEnable	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

ports [port_type]

Initiates an editing session in which to change configuration parameters for all internal ports, all external ports, or all ports based on the value given by [port_type]. port_type can be "internal" or "external". If you omit [port_type], all ports are changed. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. Press **q** to end the configuration. [Table 44](#) describes the port parameters.

security

Initiates an edit session in which to change the security settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. Press **q** or **Q** to end the editing session. [Table 45](#) describes the Set Config Security parameters.


 **IMPORTANT:** This operand is available only with the SANtegrity Enhanced PFE key.

Table 45 Security configuration parameters

Parameter	Description
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding on all switches the fabric. Fabric binding associates switch World Wide Names with a domain ID in the creation of ISL groups.
AutoSave	Enables (True) or disables (False) the saving of changes to active security set in the switch permanent memory. The default is True.

switch

Initiates an edit session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. [Table 46](#) describes the Set Config Switch parameters.

Table 46 Set Config switch parameters

Parameter	Description
AdminState	Switch administrative state: Online, Offline, or Diagnostics. The default is Online.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information. The default is True.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name for the switch. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is McDATA4GbSAN.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Default Config.
InteropMode	Interoperability mode. Choose from the following: <ul style="list-style-type: none">• Use Standard to connect to FC-SW-2 compliant switches including McDATA switches in Open Fabric Mode. This is the default.• Use the McDATA Fabric Mode to connect to McDATA switches in McDATA Fabric Mode.

threshold

Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the Config command for information about saving and activating a configuration. [Table 47](#) describes the Set Config Threshold parameters. The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Table 47 Set Config threshold parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: <ul style="list-style-type: none">• CRC errors• Decode errors• ISL connection count• Device login errors• Device logout errors• Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The switch will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The period of time in seconds in which to count events

zoning

Initiates an edit session in which to change switch zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets. [Table 48](#) describes the zoning configuration parameters.

Table 48 Set Config zoning parameters

Parameter	Description
InteropAutoSave	<p>Available only when the InteropMode parameter is Standard, this parameter enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. Refer to "InteropMode" on page 159. The default is True.</p> <p>Disabling the Autosave parameter can be useful to prevent saving zoning information when experimenting with different zoning schemes. However, leaving the Autosave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Autosave parameter should be enabled in a production environment.</p>
DefaultVisibility	<p>Available only when InteropMode is Standard, this parameter enables (All) or disables (None) communication among the switch ports/devices and the fabric in the absence of an active zone set. Refer to "InteropMode" on page 159. The default is True. This parameter takes precedence over the DefaultZone parameter when InteropMode is Standard and there is no active zone set.</p>
DefaultZone	<p>Enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set or when there is no active zone set. This parameter must have the same value throughout the fabric. If InteropMode is McDATA Fabric Mode, the DefaultZone parameter is automatically distributed throughout the fabric. If McDATA 4Gb SAN Switches are in a fabric with other M-Series directors and edge switches, and the InteropMode is Standard/Open Fabric, the DefaultZone parameter MUST be disabled (False) on the McDATA 4Gb SAN Switches for zoning to function properly.</p>
DiscardInactive	<p>Enables (True) or disables (False) the discarding of the active zone set when a new zone set is activated from another switch. The default is True.</p>

Examples The following is an example of the Set Config Port command:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit
McDATA4GbSAN (admin-config) #> set config port 0
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

Configuring Port Number: 0

AdminState	(1=Online, 2=Offline, 3=Diagnostics, 4=Down)	[Online]
LinkSpeed	(1=1Gb/s, 2=2Gb/s, 4=4Gb/s, A=Auto)	[Auto]
PortType	(GL / G / F / FL)	[GL]
SymPortName	(string, max=32 chars)	[Port0]
ALFairness	(True / False)	[False]
DeviceScanEnable	(True / False)	[True]
ForceOfflinerSCN	(True / False)	[False]
ARB_FF	(True / False)	[False]
InteropCredit	(decimal value, 0-255)	[0]
FANEnable	(True / False)	[True]
AutoPerfTuning	(True / False)	[False]
LCFEnable	(True / False)	[False]
MFSEnable	(True / False)	[False]
VIEnable	(True / False)	[False]
MSEnable	(True / False)	[True]
NoClose	(True / False)	[False]
PDISCPingEnable	(True / False)	[True]

Finished configuring attributes.

This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.

To discard this configuration use the config cancel command.

The following is an example of the Set Config Security command:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit
McDATA4GbSAN (admin-config) #> set config security
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

FabricBindingEnabled	(True / False)	[False]
AutoSave	(True / False)	[True]

Finished configuring attributes.

This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

The following is an example of the Set Config Switch command:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit
McDATA4GbSAN (admin-config) #> set config switch
```

A list of attributes with formatting and default values will follow.
Enter a new value or simply press the ENTER key to accept current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

AdminState	(1=Online, 2=Offline, 3=Diagnostics)	[Online]
BroadcastEnabled	(True / False)	[True]
InbandEnabled	(True / False)	[True]
FDMIEnabled	(True / False)	[True]
FDMIEntries	(decimal value, 0-1000)	[1000]
DefaultDomainID	(decimal value, 97-127)	[2]
DomainIDLock	(True / False)	[False]
SymbolicName	(string, max=32 chars)	[4Gb SAN Switch]	
R_A_TOV	(decimal value, 100-100000 msec)	[10000]
E_D_TOV	(decimal value, 10-20000 msec)	[2000]
PrincipalPriority	(decimal value, 1-255)	[254]
ConfigDescription	(string, max=64 chars)	[Default Config]	
InteropMode	(0=Standard, 1=McData Fabric Mode)	[Standard]

The following is an example of the Set Config Threshold command:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit
McDATA4GbSAN (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
ThresholdMonitoringEnabled      (True / False)      [False    ]

CRCErrorsMonitoringEnabled     (True / False)      [True     ]
  RisingTrigger                 (decimal value, 1-1000) [25      ]
  FallingTrigger                (decimal value, 0-1000) [1       ]
  SampleWindow                  (decimal value, 1-1000 sec) [10     ]

DecodeErrorsMonitoringEnabled  (True / False)      [True     ]
  RisingTrigger                 (decimal value, 1-1000) [200    ]
  FallingTrigger                (decimal value, 0-1000) [0      ]
  SampleWindow                  (decimal value, 1-1000 sec) [10     ]

ISLMonitoringEnabled          (True / False)      [True     ]
  RisingTrigger                 (decimal value, 1-1000) [2      ]
  FallingTrigger                (decimal value, 0-1000) [0      ]
  SampleWindow                  (decimal value, 1-1000 sec) [10     ]

LoginMonitoringEnabled         (True / False)      [True     ]
  RisingTrigger                 (decimal value, 1-1000) [5      ]
  FallingTrigger                (decimal value, 0-1000) [1      ]
  SampleWindow                  (decimal value, 1-1000 sec) [10     ]

LogoutMonitoringEnabled        (True / False)      [True     ]
  RisingTrigger                 (decimal value, 1-1000) [5      ]
  FallingTrigger                (decimal value, 0-1000) [1      ]
  SampleWindow                  (decimal value, 1-1000 sec) [10     ]

LOSMonitoringEnabled           (True / False)      [True     ]
  RisingTrigger                 (decimal value, 1-1000) [100    ]
  FallingTrigger                (decimal value, 0-1000) [5      ]
  SampleWindow                  (decimal value, 1-1000 sec) [10     ]
Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Zoning command.

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> config edit
McDATA4GbSAN (admin-config) #> set config zoning
```

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

```
InteropAutoSave      (True / False) [True ]
DefaultVisibility    (All / None)  [None ]
DefaultZone          (True / False) [False]
DiscardInactive      (True / False) [False]
```

Finished configuring attributes.

This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.

See also [Config command](#), page 118

Set Log command

Description Specifies the events to record in the event log and display on the screen. You determine what events to record in the switch event log using the Component, Level, and Port operands. You determine what events are automatically displayed on the screen using the Display operand. Alarms are always displayed on the screen.

Authority Admin session

Syntax set log
archive
clear
component [filter_list]
display [filter]
level [filter]
port [port_list]
restore
save
start (default)
stop

Operands archive

Collects all log entries and stores the result in a new file named `logfile` that is maintained in switch memory where it can be downloaded using FTP. To download `logfile`, open an FTP session, log in with account name ("images") and password ("images"), and enter "get logfile".

clear

Clears all log entries.

component [filter_list]

Specifies one or more components given by [filter_list] to monitor for events. A component is a firmware that is responsible for a particular portion of switch operation. Use a `<space>` to delimit values in the list. [filter_list] can be one or more of the following:

All

Monitors all components. To maintain optimal switch performance, do not use this setting with the Level operand set to Info.

Chassis

Monitors chassis hardware components such as fans and power supplies

Eport

Monitors all E_Ports

Mgmtserver

Monitors management server status

Nameserver

Monitors name server status

None

Monitor none of the component events

Other

Monitors other miscellaneous events

Port

Monitors all port events

SNMP

Monitors all SNMP events

Switch

Monitors switch management events

Zoning

Monitors zoning conflict events

`display [filter]`

Specifies the log events to automatically display on the screen according to the event severity levels given by [filter]. [filter] can be one of the following values:

`Critical`

Critical severity level events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

`Warn`

Warning severity level events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

`Info`

Informative severity level events. The informative level describes routine events associated with a normal fabric.

`None`

Specifies no severity levels for display on the screen

`level [filter]`

Specifies the severity level given by [filter] to use in monitoring and logging events for the specified components or ports. [filter] can be one of the following values:

`Critical`

Monitors critical events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

`Warn`

Monitors warning and critical events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

`Info`

Monitors informative, warning, and critical events. The informative level describes routine events associated with a normal fabric. This is the default severity level.

`None`

Monitors none of the severity levels

`port [port_list]`

Specifies one or more ports to monitor for events. Choose one of the following values:

`[port_list]`

Specifies port or ports to monitor. Use a <space> to delimit values in the list. Ports are numbered beginning with 0.

`All`

Specifies all ports

`None`

Disables monitoring on all ports

`restore`

Restores and saves the port, component, and level settings to the default values

`save`

Saves the log settings for the component, severity level, port, and display level. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

`start`

Starts the logging of events based on the Port, Component, and Level operands assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

`stop`

Stops logging of events

Notes In addition to critical, warn, and informative severity levels, the highest event severity level is alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen.

Set Port command

Description Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin session except for the Clear operand.

Syntax `set port [port_number]`
`bypass [alpa]`
`clear`
`enable`
`speed [transmission_speed]`
`state [state]`

Operands `[port_number]`
Specifies the port. External ports are numbered 0 and 9; internal ports are numbered 1–8.

`bypass [alpa]`
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. `[alpa]` can be a specific ALPA or the operand ALL to choose all ALPAs.

`clear`
Clears the counters on the port. This operand does not require an Admin session.

`enable`
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop

`speed [transmission_speed]`
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1
One gigabit per second

2
Two gigabits per second

4
Two gigabits per second

Auto
The port speed is automatically detected

`state [state]`
Specifies one of the following administrative states for the specified port:

Online
Places the port online. This activates and prepares the port to send data.

Offline
Places the port offline. This prevents the port from receiving signal and accepting a device login.

Diagnostics
Prepares the port for testing. This prepares the port for testing and prevents the port from accepting a device login.

Down
Disables the port by removing power from the port lasers

Set Setup command

Description Manages configuration settings for Remote Authentication Dial-In User Service (RADIUS) servers, switch services, SNMP, and system configurations.

Authority Admin session

Syntax set setup
radius
services
snmp
system

Operands radius
Prompts you in a line-by-line fashion to configure RADIUS servers for user account and device authentication. [Table 49](#) describes the RADIUS server configuration fields.

Table 49 RADIUS service settings

Entry	Description
DeviceAuthOrder	<p>IMPORTANT: This setting is valid only with the SANtegrity Enhanced PFE key</p> <p>Authenticator priority for devices:</p> <ul style="list-style-type: none">• Local — authenticate devices using only the local security database. This is the default.• Radius — authenticate devices using only the security database on the RADIUS server.• RadiusLocal — authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
UserAuthOrder	<p>Authenticator priority for user accounts:</p> <ul style="list-style-type: none">• Local — authenticate users using only the local security database. This is the default.• Radius — authenticate users using only the security database on the RADIUS server.• RadiusLocal — authenticate users using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
TotalServers	Number of RADIUS servers to configure during this session. Setting TotalServers to 0 disables all RADIUS authentication. The default is 0.
ServerIPAddress	IP address of the RADIUS server. The default is 10.0.0.1.
ServerUDPPort	User Datagram Protocol (UDP) port number on the RADIUS server. The default is 1812.
DeviceAuthServer	<p>IMPORTANT: This setting is valid only with the SANtegrity Enhanced PFE key</p> <p>Enable (True) or disable (False) this server for device authentication. The default is False.</p>

Table 49 RADIUS service settings (continued)

Entry	Description
UserAuthServer	Enable (True) or disable (False) this server for user account authentication. A user authentication RADIUS server requires a secure management connection (SSL). The default is True.
AccountingServer	Enable (True) or disable (False) this server for auditing of activity during a user session. When enabled, user activity is audited whether UserAuthServer is enabled or not. The default is False. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).
Timeout	Number of seconds to wait to receive a response from the RADIUS server before timing out. The default is 2.
Retries	Number of retries after the first attempt to establish communication with the RADIUS server fails. The default is 0.
SignPackets	Enable (True) or disable (False) the use of sign packets to protect the RADIUS server packet integrity. The default is False.
Secret	32-byte hex string or 16-byte ASCII string used as a password for authentication purposes between the switch and the RADIUS server.

services

Prompts you in a line-by-line fashion to enable or disable switch services. [Table 50](#) describes the switch service parameters. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets.



NOTE: Use caution when disabling TelnetEnabled and GUIMgmtEnabled; it is possible to disable all Ethernet access to the switch.

Table 50 Switch services settings

Entry	Description
TelnetEnabled	Enables (True) or disables (False) the ability to manage the switch over a Telnet connection. Disabling this service is not recommended. The default is True.
SSHEEnabled	Enables (True) or disables (False) Secure Shell (SSH) connections to the switch. SSH secures the remote connection to the switch. To establish a secure remote connection, your workstation must use an SSH client. The default is False.
GUIMgmtEnabled	Enables (True) or disables (False) out-of-band management of the switch with McDATA Web Server, Application Programming Interface, SNMP, and CIM. If this service is disabled, the switch can only be managed in-band. The default is True.

Table 50 Switch services settings (continued)

Entry	Description
SSLEnabled	<p>Enables (True) or disables (False) secure SSL connections for management applications including McDATA Web Server, the McDATA Web Server web applet, McDATA Web Server Application Programming Interface, and the CIM server. The default is False.</p> <ul style="list-style-type: none"> • To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. • This service must be enabled to authenticate users through a RADIUS server. • Enabling SSL automatically creates a security certificate on the switch. • To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.
EmbeddedGUIEnabled	<p>Enables (True) or disables (False) the McDATA Web Server web applet. The web applet enables you to point at a switch with an internet browser and run McDATA Web Server through the browser. This parameter is the master control for the Set Setup System command parameter, EmbeddedGUIEnabled. The default is True.</p>
SNMPEnabled	<p>Enables (True) or disables (False) the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). This parameter is the master control for the Set Setup SNMP command parameter, SNMPEnabled. The default is True.</p>
NTPEnabled	<p>Enables (True) or disables (False) the Network Time Protocol (NTP) which allows the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is False. This parameter is the master control for the Set Setup System command parameter, NTPClientEnabled. The default is False.</p>
CIMEnabled	<p>Enables (True) or disables (False) the management of the switch through third-party applications that use the Common Information Model (CIM). The default is True.</p>
FTPEnabled	<p>Enables (True) or disables (False) the File Transfer Protocol (FTP) for transferring files rapidly between the workstation and the switch. The default is True.</p>
MgmtServerEnabled	<p>Enables (True) or disables (False) the management of the switch through third-party applications that use GS-3 Management Server (MS). This parameter is the master control for the Set Config Port command parameter, MSEnable. The default is False.</p>

SNMP

Prompts you in a line-by-line fashion to change SNMP configuration settings. [Table 51](#) describes the SNMP fields. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets.

Table 51 SNMP configuration settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the switch. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (.). The default is undefined.
Location	Specifies the name of the switch location. The name can be up to 64 characters excluding #, semicolon (;), and comma (.). The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning.
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is "public".
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is "private".
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (.). The default is "public".
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

system

Prompts you in a line-by-line fashion to change system configuration settings. [Table 52](#) describes the system configuration fields. For each parameter, enter a new value or press **Enter** to accept the current value shown in brackets.

 **NOTE:** Changing the IP address will terminate all Ethernet management sessions.

Table 52 System configuration settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address. The default is 10.0.0.1.
Eth0NetworkMask	Ethernet subnet mask address. The default is 255.0.0.0.
Eth0GatewayAddress	Ethernet IP address gateway. The default is 10.0.0.254.
AdminTimeout	Amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
InactivityTimeout	Amount of time in minutes the switch waits before terminating an idle Telnet CLI session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.
NTPClientEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) client on the switch. This client enables the switch to synchronize its time with an NTP server. This feature supports NTP version 4 and is compatible with version 3. An Ethernet connection to the server is required and you must first set an initial time and date on the switch. The synchronized time becomes effective immediately. The default is False.
NTPServerAddress	The IP address of the NTP server from which the NTP client acquires the time and date. The default is 10.0.0.254.
EmbeddedGUIEnabled	Enables (True) or disables (False) the McDATA Web Server. Changing this parameter to False while the applet is running will terminate the applet. The default is True.

Examples The following is an example of the Set Setup RADIUS command:

```
McDATA4GbSAN (admin) #> set setup radius
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the attributes
for the server being processed, press 'q' or 'Q' and the ENTER key to do so.
If you wish to terminate the configuration process completely, press 'qq' or
'QQ' and the ENTER key to so do.

DeviceAuthOrder    (1=Local, 2=Radius, 3=RadiusLocal) [Local]
UserAuthOrder      (1=Local, 2=Radius, 3=RadiusLocal) [Local]
TotalServers       (decimal value, 0-5)          [1   ]

Server: 1
ServerIPAddress    (dot-notated IP Address)          [10.20.11.8]
ServerUDPPort      (decimal value)                    [1812   ]
DeviceAuthServer   (True / False)                       [True   ]
UserAuthServer     (True / False)                       [True   ]
AccountingServer   (True / False)                       [False  ]
Timeout            (decimal value, 10-30 secs)        [10     ]
Retries            (decimal value, 1-3, 0=None)        [0      ]
SignPackets        (True / False)                       [False  ]
Secret             (32 hex or 16 ASCII char value)    [***** ]
Do you want to save and activate this radius setup? (y/n): [n]
```

The following is an example of the Set Setup Services command:

```
McDATA4GbSAN (admin) #> set setup services
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
*Warning: If services are disabled, the connection to the switch may be lost.

TelnetEnabled      (True / False)                    [True ]
SSHEnabled         (True / False)                    [False]
GUIMgmtEnabled     (True / False)                    [True ]
SSLMgmtEnabled     (True / False)                    [False]
EmbeddedGUIEnabled (True / False)                    [True ]
SNMPEnabled        (True / False)                    [True ]
NTPEnabled         (True / False)                    [False]
CIMEnabled         (True / False)                    [True ]
FTPEEnabled        (True / False)                    [True ]
MgmtServerEnabled  (True / False)                    [True ]

Do you want to save and activate this services setup? (y/n): [n]
```

The following is an example of the Set Setup SNMP command:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> set setup snmp
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
Trap Severity Options
-----
unknown,emergency,alert,critical, error, warning, notify, info, debug, mark
SNMPEnabled          (True / False)          [True          ]
Contact              (string, max=64 chars)  [<sysContact undefined]
Location             (string, max=64 chars)  [sysLocation undefined]
Trap1Address         (dot-notated IP Address) [10.20.71.15   ]
Trap1Port            (decimal value)         [162           ]
Trap1Severity        (see allowed options above) [warning       ]
Trap1Version         (1 / 2)                  [2             ]
Trap1Enabled         (True / False)          [False        ]
Trap2Address         (dot-notated IP Address) [0.0.0.0       ]
Trap2Port            (decimal value)         [162           ]
Trap2Severity        (see allowed options above) [warning       ]
Trap2Version         (1 / 2)                  [2             ]
Trap2Enabled         (True / False)          [False        ]
Trap3Address         (dot-notated IP Address) [0.0.0.0       ]
Trap3Port            (decimal value)         [162           ]
Trap3Severity        (see allowed options above) [warning       ]
Trap3Version         (1 / 2)                  [2             ]
Trap3Enabled         (True / False)          [False        ]
Trap4Address         (dot-notated IP Address) [0.0.0.0       ]
Trap4Port            (decimal value)         [162           ]
Trap4Severity        (see allowed options above) [warning       ]
Trap4Version         (1 / 2)                  [2             ]
Trap4Enabled         (True / False)          [False        ]
Trap5Address         (dot-notated IP Address) [0.0.0.0       ]
Trap5Port            (decimal value)         [162           ]
Trap5Severity        (see allowed options above) [warning       ]
Trap5Version         (1 / 2)                  [2             ]
Trap5Enabled         (True / False)          [False        ]
ReadCommunity        (string, max=32 chars)  [public        ]
WriteCommunity       (string, max=32 chars)  [private       ]
TrapCommunity        (string, max=32 chars)  [public        ]
AuthFailureTrap      (True / False)          [False        ]
ProxyEnabled         (True / False)          [True         ]
```


The following is an example of the Set Setup System command:

```
McDATA4GbSAN (admin) #> set setup system
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current
value. If you wish to terminate this process before reaching the end of
the list press 'q' or 'Q' and the ENTER key to do so.
```

Eth0NetworkDiscovery	(1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)	[Static]
Eth0NetworkAddress	(dot-notated IP Address)	[10.0.0.1]
Eth0NetworkMask	(dot-notated IP Address)	[255.255.255.0]]
Eth0GatewayAddress	(dot-notated IP Address)	[10.0.0.254]
AdminTimeout	(dec value 0-1440 minutes, 0=never)	[30]
InactivityTimeout	(dec value 0-1440 minutes, 0=never)	[0]
LocalLogEnabled	(True / False)	[True]
RemoteLogEnabled	(True / False)	[False]
RemoteLogHostAddress	(dot-notated IP Address)	[10.0.0.254]
NTPClientEnabled	(True / False)	[False]
NTPServerAddress	(dot-notated IP Address)	[10.0.0.254]
EmbeddedGUIEnabled	(True / False)	[True]

Show command

Description Displays fabric, switch, and port operational information.

Authority None

Syntax show
 about
 alarm *[option]*
 audit
 broadcast
 chassis
 cimlistener *[listener_name]*
 cimsubscription *[subscription_name]*
 config *[option]*
 domains
 fabric
 fdmi *[port_wwn]*
 interface
 log *[option]*
 lsdb
 mem *[count]*
 ns *[option]*
 pagebreak
 perf *[option]*
 port *[port_number]*
 post log
 setup *[option]*
 steering *[domain_id]*
 support
 switch
 timezone
 topology
 users
 version

Operands about

Displays an introductory set of information about operational attributes of the switch. This operand is equivalent to the Version operand.

alarm *[option]*

Displays the alarm log and session display setting. If you omit *[option]*, the command displays the last 200 alarm entries. The alarm log is cleared when the switch is reset or power cycled. *[option]* has the following value:

setting

Displays the status of the parameter that controls the display of alarms in the session output stream. This parameter is set using the Set Alarm command.

audit

Displays the most recent 200 records in the administrative audit log. The audit log contains configuration and administrative changes that have been made to the switch including the originating management session and IP address.

broadcast

Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis

Displays chassis component status and temperature.

`cimlistener [listener_name]`

Displays CIM indicator services listener information for the listener given by [listener_name]. If you omit [listener_name], the command displays all listeners.

`config [option]`

Displays switch, port, and zoning configuration attributes. Refer to the Show Config command.

`domains`

Displays list of each domain and its World Wide Name in the fabric.

`fabric`

Displays list of each domain, symbolic name, World Wide Name, node IP address, and port IP address.

`fdmi [port_wwn]`

Displays detailed information about the device host bus adapter given by [port_wwn]. If you omit [port_wwn], the command displays a summary of host bus adapter information for all attached devices in the fabric. Illegal characters in the display appear as question marks (?).

`interface`

Displays the status of the active network interfaces.

`log [option]`

Displays log entries. Refer to the Show Log command. The log is cleared when the switch is reset or power cycled.

`lsdb`

Displays Link State database information.

`mem [count]`

Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.



NOTE: This operand will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

`ns [option]`

Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

`all`

Displays name server information for all switches and ports.

`[domain_id]`

Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.

`[port_id]`

Displays name server information for the port given by [port_id]. [port_id] is a port FC address.

`pagebreak`

Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

`perf [option]`

Displays performance information for all ports. Refer to the Show Perf command.

`port [port_number]`

Displays operational information for the port given by [port_number]. External ports are numbered 0 and 9; internal ports are numbered 1–8. If [port number] is omitted, information is displayed for all ports. [Table 53](#) describes the port parameters.

Table 53 Show Port parameters

Entry	Description
Alinit	Incremented each time the port begins AL initialization
AlinitError	Number of times the port entered initialization and the initialization failed
Bad Frames	Number of frames that have framing errors
ClassXFramesIn	Number of class x frames received by this port
ClassXFramesOut	Number of class x frames sent by this port
ClassXWordsIn	Number of class x words received by this port
ClassXWordsOut	Number of class x words sent by this port
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF
DecodeError	Number of decode errors detected
EpConnects	Number of times an E_Port connected through ISL negotiation
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowererrors	Received a frame when there were no available credits
FReject	Number of frames from devices that were rejected
InvalidCRC	Invalid CRC detected
InvalidDestAddr	Invalid destination address detected
LIP_AL_PD_ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed
LIP_F7_AL_PS	This LIP is used to re-initialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
Login	Number of device logins
Logout	Number of device logouts
LoopTimeouts	A two (2) second timeout as specified by FC-AL2
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
PrimSeqErrors	Primitive sequence errors detected
RxLinkResets	Number of link reset primitives received from an attached device

Table 53 Show Port parameters (continued)

Entry	Description
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port
TotalLinkResets	Total number of link reset primitives
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port
TotalRxFrames	Total number of frames received by this port
TotalRxWords	Total number of words received by this port
TotalTxFrames	Total number of frames issued by this port
TotalTxWords	Total number of words issued by this port
TxLinkResets	Number of Link Resets issued by this port
TxOfflineSeq	Total number of Offline Sequences issued by this port

`post log`

Displays the POST log which contains results from the most recently failed POST.

`setup [option]`

Displays setup attributes for the system, SNMP, and the switch manufacturer. Refer to the Set Setup command.

`steering [domain_id]`

Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

`support`

Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This operand is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Alias List
- Config List
- Date
- Group List
- History
- Ps
- Security (List, Limits, History)
- Securityset (Active, List)

- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Security, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Fabric, Log, Log Archive, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts
- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch

Displays switch operational information. [Table 54](#) describes the switch operational parameters.

Table 54 Switch operational parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch World Wide Name
SwitchType	Switch model
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	FC address of switch port 0
FlashSize - MBytes	Size of the flash memory in megabytes
LogLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch
NumberOfResets	Number of times the switch has been reset over its service life
ReasonForLastReset	Action that caused the last reset
ActiveImageVersion — build date	Active firmware image version and build date
PendingImageVersion — build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle.
ActiveConfiguration	Name of the switch configuration that is in use
AdminState	Switch administrative state
AdminModeActive	Admin session status
BeaconOnStatus	Beacon status as set by the Set Beacon command
OperationalState	Switch operational state
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
BoardTemp (1) — Degrees Celsius	Internal switch temperature at circuit board sensor 1
SwitchDiagnosticsStatus	Results of the POST
SwitchTemperatureStatus	Switch temperature status: normal, warning, failure

timezone

Displays the current time zone setting.

topology

Displays all connected devices.

users

Displays a list of logged-in users. This is equivalent to the User List command.

version

Displays an introductory set of information about operational attributes of the switch. This operand is equivalent to the About operand.

Examples The following is an example of the Show Chassis command:

```
McDATA4GbSAN #> show chassis
Chassis Information
-----
BoardTemp (1) - Degrees Celsius    31
PowerSupplyStatus (1)              Good
HeartBeatCode                      1
HeartBeatStatus                    Normal
```

The following is an example of the Show Domains command:

```
McDATA4GbSAN #> show domains
Principal switch is (remote): 10:00:00:60:69:50:0b:6c
Upstream Principal ISL is      : 1
Domain ID List:
  Domain 97 (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
  Domain 98 (0x62)  WWN = 10:00:00:60:df:22:2e:0c
  Domain 99 (0x63)  WWN = 10:00:00:c0:dd:00:72:45
  Domain 100 (0x64) WWN = 10:00:00:c0:dd:00:ba:68
  Domain 101 (0x65) WWN = 10:00:00:60:df:22:2e:06
  Domain 102 (0x66) WWN = 10:00:00:c0:dd:00:90:ef
  Domain 103 (0x67) WWN = 10:00:00:60:69:50:0b:6c
  Domain 104 (0x68) WWN = 10:00:00:c0:dd:00:b8:b7
```

The following is an example of the Show Fabric command:

```
McDATA4GbSAN #> show fabric
```

Domain	WWN	Enet IP Addr	FC IP Addr	SymbolicName
-----	---	-----	-----	-----
16 (0x10)	10:00:00:c0:dd:00:77:81	10.20.68.11	0.0.0.0	gui sb1 .11
17 (0x11)	10:00:00:c0:dd:00:6a:2d	10.20.68.12	0.0.0.0	sw12
18 (0x12)	10:00:00:c0:dd:00:c3:04	10.20.68.160	0.0.0.0	sw .160
19 (0x13)	10:00:00:c0:dd:00:bc:56	10.20.68.108	0.0.0.0	Sb2 .108

The following is an example of the Show FDMI command:

```
McDATA4GbSAN #> show fdmi
```

HBA ID	PortID	Manufacturer	Model	Ports
-----	-----	-----	-----	-----
21:01:00:e0:8b:27:aa:bc	610000	QLogic Corporation	QLA2342	2
21:00:00:00:ca:25:9b:96	180100	QLogic Corporation	QL2330	2

The following is an example of the Show FDMI WWN command:

```
McDATA4GbSAN #> show fdmi 21:00:00:e0:8b:09:3b:17
FDMI Information
-----
Manufacturer           QLogic Corporation
SerialNumber            [04202
Model                   QLA2342
ModelDescription        QLogic QLA2342 PCI Fibre Channel Adapter
PortID                  610000
NodeWWN                 20:00:00:e0:8b:07:aa:bc
HardwareVersion         FC5010409-10
DriverVersion           8.2.3.10 Beta 2 (W2K VI)
OptionRomVersion        1.21
FirmwareVersion         03.02.13.
OperatingSystem         SunOS 5.8
MaximumCTPayload        2040
NumberOfPorts           1

Port 21:01:00:e0:8b:27:aa:bc

SupportedFC4Types       FCP
SupportedSpeed           2Gb/s
CurrentSpeed             2Gb/s
MaximumFrameSize        2048
OSDeviceName
HostName
```

The following is an example of the Show NS (local domain) command:

```
McDATA4GbSAN #> show ns
Seq Domain      Port      Port
No  ID          ID        Type COS PortWWN          NodeWWN
---  -
1   98 (0x62) 620100 N    3   50:05:08:b2:00:7b:a7:e2 50:05:08:b2:00:7b:a7:e0
2   98 (0x62) 620200 N    3   50:05:08:b2:00:7c:6e:22 50:05:08:b2:00:7c:6e:20
3   98 (0x62) 620300 N    3   50:05:08:b2:00:7c:60:b2 50:05:08:b2:00:7c:60:b0
4   98 (0x62) 620400 N    3   50:05:08:b2:00:7c:5b:92 50:05:08:b2:00:7c:5b:90
5   98 (0x62) 620500 N    3   50:05:08:b2:00:74:d0:92 50:05:08:b2:00:74:d0:90
6   98 (0x62) 620600 N    3   50:05:08:b2:00:7c:30:82 50:05:08:b2:00:7c:30:80
7   98 (0x62) 620700 N    3   50:05:08:b2:00:7c:52:12 50:05:08:b2:00:7c:52:10
8   98 (0x62) 620800 N    3   50:05:08:b2:00:7d:f1:32 50:05:08:b2:00:7d:f1:30
```

The following is an example of the Show NS [port_ID] command:

```
McDATA4GbSAN #> show ns 1301e1
Port ID: 620100
-----
PortType           N
PortWWN            50:05:08:b2:00:7b:a7:e2
SymbolicPortName   (NULL)
NodeWWN            50:05:08:b2:00:7b:a7:e0
SymbolicNodeName   QLA2312 FW:v3.02.28 DVR:v9.0.0.13 (w32 IP)
NodeIPAddress      0.0.0.0
ClassOfService     3
PortIPAddress      0.0.0.0
FabricPortName     20:01:08:00:88:e0:aa:b5
FC4Type            FCP
FC4Desc            (NULL)
```


The following is an example of the Show Interface command:

```
McDATA4GbSAN #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:BD:ED
          inet addr:10.20.68.107  Bcast:10.20.68.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

The following is an example of the Show Port command:

```
McDATA4GbSAN #> show port 0
Port Number: 0
-----
AdminState      Online          PerfTuningMode  Normal
AsicNumber      0              PortID          620000
AsicPort        8              PortWWN         20:00:08:00:88:e0:aa:b5
ConfigType      GL             RunningType     Unknown
DiagStatus      Passed         MediaPartNumber FTRJ8524P2BNL
EpConnState     None          MediaRevision   A
EpIsoReason     NotApplicable MediaType        400-M5-SN-I
LinkSpeed       Auto          MediaVendor     FINISAR CORP.
LinkState       Inactive      MediaVendorID   00009065
LoginStatus     NotLoggedIn   SymbolicName    Port0
MaxCredit       8             SyncStatus      SyncLost
MediaSpeeds     1Gb/s, 2Gb/s, 4Gb/s XmitterEnabled True
OperationalState Offline

ALInit          1              LIP_F8_AL_PS   0
ALInitError     0              LIP_F8_F7      0
BadFrames       0              LinkFailures   0
Class2FramesIn  0              Login          0
Class2FramesOut 0              Logout         0
Class2WordsIn   0              LoopTimeouts   0
Class2WordsOut  0              LossOfSync     0
Class3FramesIn  0              PrimSeqErrors  0
Class3FramesOut 0              RxLinkResets   0
Class3Toss      0              RxOfflineSeq   0
Class3WordsIn   0              TotalErrors    0
Class3WordsOut  0              TotalLinkResets 0
DecodeErrors    0              TotalLIPsRecvd 0
EpConnects     0              TotalLIPsXmitd 1
FBusy          0              TotalOfflineSeq 1
FlowErrors      0              TotalRxFrames  0
FReject         0              TotalRxWords   0
InvalidCRC      0              TotalTxFrames  0
InvalidDestAddr 0              TotalTxWords   0
LIP_AL_PD_AL_PS 0              TxLinkResets   0
LIP_F7_AL_PS   0              TxOfflineSeq    1
LIP_F7_F7      0
```

The following is an example of the Show Switch command:

```
McDATA4GbSAN #> show switch
Switch Information
-----
SymbolicName                McDATA4GbSAN
SwitchWWN                   10:00:08:00:88:e0:aa:b5
BootVersion                  V1.3.0.8.0 (Tue Mar  8 10:24:41 2005)
CreditPool                  0
DomainID                    98 (0x62)
FirstPortAddress            620000
FlashSize - MBytes         128
LogFilterLevel              Info
MaxPorts                    10
NumberOfResets              4
ReasonForLastReset          HotReset
ActiveImageVersion - build date V5.2.0.19.6 (Mon Mar 28 03:26:05 2005)
PendingImageVersion - build date V5.2.0.19.6 (Mon Mar 28 03:26:05 2005)
ActiveConfiguration         default
AdminState                  Online
AdminModeActive             False
BeaconOnStatus              False
OperationalState            Online
PrincipalSwitchRole         True
BoardTemp (1) - Degrees Celsius 41
SwitchDiagnosticsStatus     Passed
SwitchTemperatureStatus     Normal
```

The following is an example of the Show Topology command:

```
McDATA4GbSAN #> show topology
Unique ID Key
-----
A = ALPA, D = Domain ID, P = Port ID
```

Port	Loc Type	Local PortWWN	Rem Type	Remote NodeWWN	Unique ID	
----	----	-----	----	-----	-----	
Int:1	F	20:01:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7b:a7:e0	620100	P
Int:2	F	20:02:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7c:6e:20	620200	P
Int:3	F	20:03:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7c:60:b0	620300	P
Int:4	F	20:04:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7c:5b:90	620400	P
Int:5	F	20:05:08:00:88:e0:aa:b5	N	50:05:08:b2:00:74:d0:90	620500	P
Int:6	F	20:06:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7c:30:80	620600	P
Int:7	F	20:07:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7c:52:10	620700	P
Int:8	F	20:08:08:00:88:e0:aa:b5	N	50:05:08:b2:00:7d:f1:30	620800	P

The following is an example of the Show Topology command for port 10:

```
McDATA4GbSAN #> show topology 1
Local Link Information
-----

Port          Int:1
PortID        620100
PortWWN       20:01:08:00:88:e0:aa:b5
PortType      F

Remote Link Information
-----

Device 0

PortID        620100
PortWWN       50:05:08:b2:00:7b:a7:e2
NodeWWN       50:05:08:b2:00:7b:a7:e0
PortType      N
Description   (NULL)
IPAddress     0.0.0.0
```

The following is an example of the Show Version command:

```
McDATA4GbSAN #> show version
*****
*
*          Command Line Interface SHell   (CLISH)
*
*****

SystemDescription   McDATA 4Gb SAN Switch
Eth0NetworkAddress  10.20.94.50 (use 'set setup system' to update)
MACAddress           00:c0:dd:07:12:1b
WorldWideName        10:00:08:00:88:e0:aa:b5
ChassisSerialNumber  0508a00172
SymbolicName         McDATA4GbSAN
ActiveSWVersion      V5.2.0.19.6
ActiveTimestamp      Mon Mar 28 03:26:05 2005
DiagnosticsStatus    Passed
ISLLicensedPorts    All
```

See also [Show Config command](#), page 188

[Show Log command](#), page 191

[Show Perf command](#), page 194

[Show Setup command](#), page 196

Show Config command

Description Displays switch, port, alarm threshold, security, and zoning for the current configuration.

Authority None

Syntax show config
port [port_number]
security
switch
threshold
zoning

Operands port [port_number]
Displays configuration parameters for the port number given by [port_number]. External ports are numbered 0 and 9; internal ports are numbered 1–8. If [port_number] is omitted, all ports are specified.

security
Displays the security database Autosave parameter value.

switch
Displays configuration parameters for the switch.

threshold
Displays alarm threshold parameters for the switch.

zoning
Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
McDATA4GbSAN #> show config port 9
Configuration Name: default
-----
Port Number: 9
-----
AdminState           Online
LinkSpeed            Auto
PortType              GL
SymbolicName         Port9
ALFairness           False
DeviceScanEnabled    True
ForceOfflineRSCN     False
ARB_FF               False
InteropCredit        0
FANEnabled           True
AutoPerfTuning       True
MSEnabled            True
NoClose              False
PDISCPingEnabled     True
MSEnabled            True
NoClose              False
PDISCPingEnabled     True
```

The following is an example of the Show Config Switch command:

```
McDATA4GbSAN #> show config switch
Configuration Name: default
-----
AdminState           Online
BroadcastEnabled     True
InbandEnabled        True
FdmEnabled           True
FdmEntries           1000
DefaultDomainID      98 (0x62)
DomainIDLck          False
SymbolicName         McDATA4GbSAN
R_A_TOV              10000
E_D_TOV              2000
PrincipalPriority     254
ConfigDescription    Default Config
ConfigLastSavedBy    Initial
ConfigLastSavedOn    Initial
InteropMode          Standard
```

The following is an example of the Show Config Threshold command:

```
McDATA4GbSAN #> show config threshold
Configuration Name: default
-----
Threshold Configuration Information
-----
ThresholdMonitoringEnabled  False
CRCErrorsMonitoringEnabled  True
  RisingTrigger              25
  FallingTrigger             1
  SampleWindow               10
DecodeErrorsMonitoringEnabled True
  RisingTrigger              25
  FallingTrigger             0
  SampleWindow               10
ISLMonitoringEnabled       True
  RisingTrigger              2
  FallingTrigger             0
  SampleWindow               10
LoginMonitoringEnabled     True
  RisingTrigger              5
  FallingTrigger             1
  SampleWindow               10
LogoutMonitoringEnabled    True
  RisingTrigger              5
  FallingTrigger             1
  SampleWindow               10
LOSMonitoringEnabled       True
  RisingTrigger              100
  FallingTrigger             5
  SampleWindow               10
```

The following is an example of the Show Config Zoning command:

```
McDATA4GbSAN #> show config zoning
Configuration Name: default
-----
Zoning Configuration Information
-----
InteropAutoSave      True
DefaultVisibility    None
DefaultZone          False
DiscardInactive      False
```

See also [Set Config command](#), page 156

Show Log command

Description Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax show log
[number_of_events]
component
display [filter]
level
options
port
settings

Operands [number_of_events]
Specifies the number of the most recent events to display from the event log. [number_of_events] must be a positive integer.

component

Displays the components currently being monitored for events. The components are as follows:

All

Monitors all components

Chassis

Monitors chassis hardware components such as fans and power supplies

Eport

Monitors all E_Ports

Mgmtserver

Monitors management server status

Nameserver

Monitors name server status

None

Monitor none of the component events

Other

Monitors other miscellaneous events

Port

Monitors all port events

SNMP

SNMP events

Switch

Monitors switch management events

Zoning

Monitors zoning conflict events

display [filter]

Displays log events on the screen according to the component or severity level filter given by [filter]. [filter] can be one of the following:

Info

Displays all informative events

Warning

Displays all warning events

Critical

Displays all critical events

Eport

Displays all events related to E_Ports

Mgmtserver

Displays all events related to the management server

Nameserver

Displays all events related to the name server

Port [port_number]

Displays all events related to the port given by [port_number]. External ports are numbered 0 and 9; internal ports are numbered 1–8.

SNMP

Displays all events related to SNMP

Switch

Displays all events related to switch management

Zoning

Displays all events related to zoning

level

Displays the event severity level logging setting and the display level setting

options

Displays the options that are available for configuring event logging and automatic display to the screen. Refer to the for information about how to configure event logging and display level.

port

Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings

Displays the current filter settings for component, severity level, port, and display level. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples The following is an example of the Show Log Component command:

```
McDATA4GbSAN #> show log component
```

```
Current settings for log
```

```
-----
```

```
FilterComponent  NameServer MgmtServer Zoning Switch Blade Port Eport Snmp
```

The following is an example of the Show Log Level command:

```
McDATA4GbSAN #> show log level
```

```
Current settings for log
```

```
-----
```

```
FilterLevel      Info
```

```
DisplayLevel     Critical
```


The following is an example of the Show Log Options command:

```
McDATA4GbSAN #> show log options
  Allowed options for log
  -----
  FilterComponent
  All, None, NameServer, MgmtServer, Zoning, Switch, Blade, Port, Eport, Snmp
  FilterLevel      Critical, Warn, Info, None
  DisplayLevel     Critical, Warn, Info, None
```

The following is an example of the Show Log command:

```
McDATA4GbSAN #> show log
[327][day month date time year][I][Eport Port:0/8][Eport State=
E_A0_GET_DOMAIN_ID]
[328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
[329][day month date time year][I][Eport Port: 0/8][Sending init hello]
[330][day month date time year][I][Eport Port: 0/8][Processing EFP,oxid= 0x8]
[331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
[332][day month date time year][I][Eport Port: 0/8][EFP,WWN=
0x100000c0dd00b845,len= 0x30]
[333][day month date time year][I][Eport Port: 0/8][Sending LSU
oxid=0xc:type=1]
[334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
[335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
[336][day month date time year][I][Eport Port: 0/8][Setting attribute
Oper.UserPort.0.8.EpConnState Connected]
```

See also [Set Log command](#), page 166

Show Perf command

Description Displays port performance in frames/second and bytes/second. If you omit the operand, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority None

Syntax show perf
byte
inbyte
outbyte
frame
inframe
outframe
errors

Operands byte
Displays continuous performance data in total bytes/second transmitted and received. Press any key to stop the display.

inbyte
Displays continuous performance data in bytes/second received. Press any key to stop the display.

outbyte
Displays continuous performance data in bytes/second transmitted. Press any key to stop the display.

frame
Displays continuous performance data in total frames/second transmitted and received. Press any key to stop the display.

inframe
Displays continuous performance data in frames/second received. Press any key to stop the display.

outframe
Displays continuous performance data in frames/second transmitted. Press any key to stop the display.

errors
Displays continuous error counts. Press any key to stop the display.

Examples The following is an example of the Show Perf command:

```
McDATA4GbSAN #> show perf
      Bytes/s   Bytes/s   Bytes/s   Frames/s   Frames/s   Frames/s
      Port     (in)      (out)     (total)   (in)      (out)     (total)
      ----     -
Ext:0  21M       0         21M       24K        0         24K
Ext:9  85K       20M       20M       108        12K       12K

Int:1  1K        4M        4M        32         2K        2K
Int:2  0         0         0         0          0         0
Int:3  1K        4M        4M        33         2K        2K
Int:4  0         0         0         0          0         0
Int:5  0         0         0         0          0         0
Int:6  278K     327K     605K     216        423       639
Int:7  0         0         0         0          0         0
Int:8  0         0         0         0          0         0
```

The following is an example of the Show Perf Byte command:

```
McDATA4GbSAN #> show perf byte
Displaying bytes/sec (total)... (Press any key to stop display)
```

0	9	1	2	3	4	5	6	7	8
30M	12M	43M	5M	0	4M	0	0	818K	0
17M	17M	35M	4M	0	4M	0	0	733K	0
20M	20M	40M	5M	0	5M	0	0	902K	0
45M	11M	56M	3M	0	4M	0	0	465K	0
20M	20M	41M	4M	0	4M	0	0	728K	0
19M	19M	39M	4M	0	5M	0	0	911K	0
45M	11M	56M	4M	0	4M	0	0	536K	0
20M	20M	41M	4M	0	3M	0	0	458K	0
19M	19M	38M	3M	0	3M	0	0	703K	0
45M	11M	56M	5M	0	5M	0	0	626K	0
21M	20M	41M	4M	0	4M	0	0	1M	0
20M	20M	40M	4M	0	4M	0	0	1M	0
44M	10M	55M	4M	0	4M	0	0	1M	0
21M	20M	41M	4M	0	4M	0	0	399K	0

Show Setup command

Description Displays the current SNMP and system settings.

Authority None

Syntax show setup
mfg
radius
services
snmp
system

Operands mfg
Displays manufacturing information about the switch.

radius
Displays RADIUS server information.

services
Displays switch service status information.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
McDATA4GbSAN #> show setup mfg
Manufacturing Information
-----
BrandName           McDATA
BuildDate           Unknown
ChassisPartNumber   BRS-482M11
ChassisSerialNumber 0508a00172
CPUBoardSerialNumber 0508a00172
MACAddress          00:c0:dd:07:12:1b
PlanarPartNumber    Unknown
SwitchSymbolicName  McDATA4GbSAN
SwitchWWN           10:00:08:00:88:e0:aa:b5
SystemDescription   McDATA 4Gb SAN Switch
SystemObjectID      1.3.6.1.4.1.1663.1.1.1.1.37
```

The following is an example of the Show Setup Services command:

```
McDATA4GbSAN #> show setup services
System Services
-----
TelnetEnabled       True
SSHEnabled          False
GUIMgmtEnabled      True
SSLMgmtEnabled      False
EmbeddedGUIEnabled  True
SNMPEnabled         True
NTPEnabled          True
CIMEnabled          True
FTPEnabled          True
MgmtServerEnabled   True
```

The following is an example of the Show Setup RADIUS command:

```
McDATA4GbSAN #> show setup radius
```

```
Radius Information
-----
DeviceAuthOrder  RadiusLocal
UserAuthOrder    RadiusLocal
TotalServers     1

Server: 1

ServerIPAddress  10.20.11.8
ServerUDPPort    1812
DeviceAuthServer False
UserAuthServer   True
AccountingServer False
Timeout          2
Retries          0
SignPackets      False
Secret           *****
```

The following is an example of the Show Setup Snmp command:

```
McDATA4GbSAN #> show setup snmp
```

```
SNMP Information
-----
SNMPEnabled      True
Contact          <sysContact undefined>
Location         System Lab
Description      McDATA 4Gb SAN Switch
Trap1Address     10.0.0.254
Trap1Port        162
Trap1Severity    warning
Trap1Version     2
Trap1Enabled     False
Trap2Address     0.0.0.0
Trap2Port        162
Trap2Severity    warning
Trap2Version     2
Trap2Enabled     False
Trap3Address     0.0.0.0
Trap3Port        162
Trap3Severity    warning
Trap3Version     2
Trap3Enabled     False
Trap4Address     0.0.0.0
Trap4Port        162
Trap4Severity    warning
Trap4Version     2
Trap4Enabled     False
Trap5Address     0.0.0.0
Trap5Port        162
Trap5Severity    warning
Trap5Version     2
Trap5Enabled     False
ObjectID         1.3.6.1.4.1.1663.1.1.1.1.37
AuthFailureTrap  True
ProxyEnabled     True
```

The following is an example of the Show Setup System command:

```
McDATA4GbSAN #> show setup system
System Information
-----
Eth0NetworkDiscovery      Static
Eth0NetworkAddress       10.20.92.246
Eth0NetworkMask          255.255.255.0
Eth0GatewayAddress       10.20.92.1
AdminTimeout              30
InactivityTimeout        0
LocalLogEnabled           True
RemoteLogEnabled          False
RemoteLogHostAddress     10.0.0.254
NTPClientEnabled         False
NTPServerAddress         10.0.0.254
EmbeddedGUIEnabled       True
```

See also [Set Setup command](#), page 170

Shutdown command

Description Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin session

Syntax shutdown

Test command

Description Tests ports using internal (SerDes level), external (transceiver), and online loopback tests. Internal and external tests require that the port be placed in diagnostic mode. Refer to the Set Port State command for information about changing the port administrative state. While the test is running, the remaining ports on the switch remain fully operational.

Authority Admin session

Syntax test
port [port_number] [test_type]
cancel
status

Operands port [port_number] [test_type]
Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

internal
Tests the SerDes for all port speeds independent of the capabilities of the transceiver. This is the default. The port must be in diagnostics mode to perform this test. This test is valid for all ports. External ports are 0 and 9; internal ports are numbered 1–8.

external
Tests both the SerDes and transceiver for all port speeds that are supported by the transceiver. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the transceiver. This test is valid for external ports 0 and 9.

online
Tests communications between the port and its device node or device loop at the operating port speed. The port being tested must be online and connected to a remote device. The port passes if the test frame that was sent by the switch matches the frame that is received. This test does not disrupt communication on the port. This test is valid for all ports. External ports are numbered 0 and 9; internal ports are numbered 1–8.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run an internal or external port test, perform the following procedure:

1. Enter the following command and press **Enter** to start an Admin session.

```
admin start
```
2. Enter the following command (x = port number) and press **Enter** to place the port in Diagnostics mode.

```
set port x state diagnostics
```
3. Choose the type of port loopback test to run. Enter the following command to run an internal loopback test and press **Enter**.

```
test port x internal
```

Enter the following command and press **Enter** to run an external loopback test. A loopback plug must be installed for this test to pass.

```
test port x external
```
4. A series of test parameters are displayed on the screen. Press **Enter** to accept each default parameter value, or enter a new value for each parameter and press **Enter**. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.
5. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.
6. After the test is run, put the port back into online state. Enter the following command (x = port number) and press **Enter**.

```
set port x state online
```
7. Enter the following command and press **Enter** to verify port is back online. The contents of the **AdminState** field should display to be "Online".

```
show port x
```

The online loopback (node-to-node) test requires that port be online and connected to a remote device. To run the online loopback test, perform the following procedure:

1. To start an Admin session, enter the following command and press **Enter**.

```
admin start
```
2. To run the online loopback test, enter the following command and press **Enter**.

```
test port x online
```
3. A series of test parameters are displayed on the screen. Press **Enter** to accept each default parameter value, or enter a new value for each parameter and press **Enter**. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

```
McDATA4GbSAN (admin) #> test port x online
```

A list of attributes with formatting and current values will follow. Enter a new value or simply press the ENTER key to accept the default value. If you wish to terminate this process before reaching the end of the list press 'q' or 'Q' and the ENTER key to do so.

```
TestLength      (decimal value, 1-4294967295)  [100   ]
FrameSize       (decimal value, 36-2148)             [256   ]
DataPattern     (32-bit hex value or 'Default') [Default]
StopOnError     (True/False)                       [False ]
Do you want to start the test? (y/n) [n]
```
4. After all parameter values are defined, press **Y** to start the test. After the command executes, a message on the screen will appear detailing the test results.

See also [Set command](#), page 154

Uptime command

Description Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax uptime

Examples The following is an example of the Uptime command:

```
McDATA4GbSAN #> uptime
```

```
Elapsed up time : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)  
Reason last reset: NormalReset
```

User command

Description Administers and displays user accounts.

Authority Admin account name and an Admin session. The Accounts and List operands are available to all account names without an Admin session.

Syntax user
accounts
add
delete [account_name]
edit
list

Operands accounts
Displays all user accounts that exist on the switch. This operand is available to all account names without an Admin session.

add

Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 8–20 characters.
- Admin authority grants permission to use the Admin command to open an Admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]

Deletes the account name given by [account_name] from the switch.

edit

Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list

Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This operand is available to all account names without an Admin session.

Notes Authority level or password changes that you make to an account that is currently logged in do not take effect until that account logs in again.

Examples The following is an example of the User Accounts command:

```
McDATA4GbSAN (admin) #> user accounts
```

```
Current list of user accounts
```

```
-----
```

```
images      (admin authority = False, never expires)
admin       (admin authority = True , never expires)
chuckca     (admin authority = False, expires in < 50 days)
gregj       (admin authority = True , expires in < 100 days)
fred        (admin authority = True , never expires)
```

The following is an example of the User Add command:

```
McDATA4GbSAN (admin) #> user add
  Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *****

please confirm account password: *****

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
McDATA4GbSAN (admin) #> user edit

  Press 'q' and the ENTER key to abort this command.

account name (1-15 chars)      : user1
set account expiration in days (0-2000, 0=never): [0]
should this account have admin authority? (y/n): [n]

OK to modify user account 'user1' with no admin authority
and to expire in 0 days?

Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
McDATA4GbSAN (admin) #> user del user3

The user account will be deleted. Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
McDATA4GbSAN (admin) #> user list
```

User	Ethernet Addr-Port	Logged in Since
admin@OB-session1	10.20.68.108-1031	day month date time year
admin@OB-session2	10.20.68.108-1034	day month date time year
snmp@OB-session3	Unknown	day month date time year
snmp@IB-session4	Unknown	day month date time year
admin@OB-session5	Unknown	day month date time year

See also [Passwd command](#), page 140

Whoami command

Description Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax whoami

Examples The following is an example of the Whoami command:

```
McDATA4GbSAN #> whoami

User name      : admin@session2
Switch name    : McDATA4GbSAN
Switch domain ID: 21 (0x15)
```

Zone command

Description Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. Refer to the Zoning command for information about starting a Zoning Edit session. The List, Members, and Zonesets operands are available without an Admin session.

Syntax zone
add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [member_list]
rename [zone_old] [zone_new]
type [zone] [zone_type]
zonesets [zone]

Operands add [zone] [member_list]

Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 97-127; port numbers can be 0–255.
- 16-character hexadecimal world wide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]

Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]

Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, \$, ^, and -. The zoning database supports a maximum of 2000 zones.

delete [zone]

Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list

Displays a list of all zones and the zone sets of which they are components. This operand does not require an Admin session.

members [zone]

Displays all members of the zone given by [zone]. This operand does not require an Admin session.

`remove [zone] [member_list]`

Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 97–127; port numbers can be 0–255.
- 16-character hexadecimal world wide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

`rename [zone_old] [zone_new]`

Renames the zone given by [zone_old] to the zone given by [zone_new].

`type [zone] [zone_type]`

Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone].

[zone_type] can only be the following type:

`soft`

Name server zone

`zonesets [zone]`

Displays all zone sets of which the zone given by [zone] is a component. This operand does not require an Admin session.

Examples The following is an example of the Zone List command:

```
McDATA4GbSAN #> zone list
```

```
Zone          ZoneSet
-----
wn_b0241f
                zone_set_1

wn_23bd31
                zone_set_1

wn_221416
                zone_set_1

wn_2215c3
                zone_set_1

wn_0160ed
                zone_set_1

wn_c001b0
                zone_set_1

wn_401248
                zone_set_1

wn_02402f
                zone_set_1

wn_22412f
                zone_set_1
```

The following is an example of the Zone Members command:

```
McDATA4GbSAN #> zone members wwn_b0241f

Current List of Members for Zone: wwn_b0241f
-----
50:06:04:82:bf:d2:18:c2
50:06:04:82:bf:d2:18:d2
21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
McDATA4GbSAN #> zone zonesets zone1

Current List of ZoneSets for Zone: zone1
-----
zone_set_1
```

See also [Zoneset command](#), page 209

[Zoning command](#), page 211

Zoneset command

Description Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the Zoning command for information about starting a Zoning Edit session. The Active, List, and Zones operands are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate operands.

Syntax

```
zoneset
  activate [zone_set]
  active
  add [zone_set] [zone_list]
  copy [zone_set_source] [zone_set_destination]
  create [zone_set]
  deactivate
  delete [zone_set]
  list
  remove [zone_set] [zone_list]
  rename [zone_set_old] [zone_set_new]
  zones [zone_set]
```

Operands activate [zone_set]
Activates the zone set given by [zone_set]. This operand deactivates the active zone set. End the Zoning Edit session before using this operand.

active
Displays the name of the active zone set. This operand does not require Admin session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]
Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0–9, A–Z, a–z, _, \$, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. End the Zoning Edit session before using this operand.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list
Displays a list of all zone sets. This operand does not require an Admin session.

remove [zone_set] [zone_list]
Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]
Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]

Displays all zones that are components of the zone set given by [zone_set]. This operand does not require an Admin session.

- Notes**
- A zone set must be active for its definitions to be applied to the fabric.
 - Only one zone set can be active at one time.
 - A zone can be a component of more than one zone set.

Examples The following is an example of the Zoneset Active command:

```
McDATA4GbSAN #> zoneset active
```

```
ActiveZoneSet      Bets
LastActivatedBy    admin@OB-session6
LastActivatedOn    day month date time year
```

The following is an example of the Zoneset List command:

```
McDATA4GbSAN #> zoneset list
```

```
Current List of ZoneSets
-----
alpha
beta
```

The following is an example of the Zoneset Zones command:

```
McDATA4GbSAN #> zoneset zones ssss
```

```
Current List of Zones for ZoneSet: ssss
-----
zone1
zone2
zone3
```

See also [Zone command](#), page 206
[Zoneset command](#), page 209

Zoning command

Description Starts a Zoning Edit session in which to create and manage zone sets and zones. Refer to the Zone command and the Zoneset command.


Authority Admin session except for the Active, History, Limits, and List operands. The Clear operand also requires a zoning edit session.

Syntax zoning
 active
 cancel
 clear
 edit
 history
 limits
 list
 restore
 save

Operands active
 Displays information for the active zone set including component zones and zone members. This operand does not require an Admin session.

cancel
 Ends the current Zoning Edit session. Any unsaved changes are lost.

clear
 Clears all inactive zone sets from the volatile edit copy of the zoning database. This operand requires a zoning edit session. This operand does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

 **NOTE:** The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

edit
 Starts a Zoning Edit session.

history
 Displays a history of zoning modifications. This operand does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits

Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This operand also displays the switch zoning database limits, excluding the active zone set, which are described in [Table 55](#). This operand does not require an Admin session.

Table 55 Zoning database limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (1)
MaxZones	Maximum number of zones (2000)
MaxAliases	Maximum number of aliases (2500)
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding those in the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

list

Lists all zoning definitions. This operand does not require an Admin session.

restore

Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save

Saves changes made during the current Zoning Edit session. The system informs you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples The following is an example of the Zoning Edit command:

```
McDATA4GbSAN #> admin start
McDATA4GbSAN (admin) #> zoning edit
McDATA4GbSAN (admin-zoning) #>
.
.
McDATA4GbSAN (admin-zoning) #> zoning cancel

Zoning edit mode will be canceled. Please confirm (y/n): [n] y

McDATA4GbSAN (admin) #> admin end
```

The following is an example of the Zoning Limits command:

```
McDATA4GbSAN #> zoning limits
```

Zoning Attribute	Maximum	Current	[Zoning Name]
-----	-----	-----	-----
MaxZoneSets	1	1	
MaxZones	2000	17	
MaxAliases	2500	1	
MaxTotalMembers	10000	166f	
MaxZonesInZoneSets	2000	19	
MaxMembersPerZone	2000	10	D_1_JBOD_1
		23	D_1_Photons
		9	D_2_JBOD1
		16	D_2_NewJBOD_2
		5	E1JBOD1
		5	E2JBOD2
		3	LinkResetZone
		3	LinkResetZone2
		8	NewJBOD1
		8	NewJBOD2
		24	Q_1Photon1
		8	Q_1_NewJBOD1
		13	Q_1_Photon_1
		21	Q_2_NewJBOD2
		3	ZoneAlias
		3	ZoneDomainPort
		4	ZoneFCAddr
MaxMembersPerAlias	2000	2	AliasInAZone

The following is an example of the Zoning Limits command:

```
McDATA4GbSAN #> zoning limits
```

Zoning Attribute	Maximum	Current	[Zoning Name]
-----	-----	-----	-----
MaxZoneSets	1	1	
MaxZones	2000	17	
MaxAliases	2500	1	
MaxTotalMembers	10000	166f	
MaxZonesInZoneSets	2000	19	
MaxMembersPerZone	2000	10	D_1_JBOD_1
		23	D_1_Photons
		9	D_2_JBOD1
		16	D_2_NewJBOD_2
		5	E1JBOD1
		5	E2JBOD2
		3	LinkResetZone
		3	LinkResetZone2
		8	NewJBOD1
		8	NewJBOD2
		24	Q_1Photon1
		8	Q_1_NewJBOD1
		13	Q_1_Photon_1
		21	Q_2_NewJBOD2
		3	ZoneAlias
		3	ZoneDomainPort
		4	ZoneFCAddr
MaxMembersPerAlias	2000	2	AliasInAZone

The following is an example of the Zoning List command:

```
McDATA4GbSAN #> zoning list
Active ZoneSet Information
ZoneSet      Zone      ZoneMember
-----
wnn
             wwn_b0241f
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                21:00:00:e0:8b:02:41:2f
             wwn_23bd31
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                10:00:00:00:c9:23:bd:31
             wwn_221416
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                10:00:00:00:c9:22:14:16
             wwn_2215c3
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                10:00:00:00:c9:22:15:c3

Configured Zoning Information
ZoneSet      Zone      ZoneMember
-----
wnn
             wwn_b0241f
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                21:00:00:e0:8b:02:41:2f
             wwn_23bd31
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                10:00:00:00:c9:23:bd:31
             wwn_221416
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                10:00:00:00:c9:22:14:16
             wwn_2215c3
                50:06:04:82:bf:d2:18:c2
                50:06:04:82:bf:d2:18:d2
                10:00:00:00:c9:22:15:
```

See also [Zone command](#), page 206
[Zoneset command](#), page 209

Glossary

Active zone set	The zone set that defines the current zoning for the fabric
Active firmware	The firmware image on the switch that is in use
Activity LED	A port LED that indicates when frames are entering or leaving the port
Administrative state	State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the Command Line Interface (CLI).
Alarm	A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.
Alias	A named set of ports or devices. An alias is not a zone, and can not have a zone or another alias as a member.
AL_PA	Arbitrated Loop Physical Address
Arbitrated loop	An FC topology where ports use arbitration to establish a point-to-point circuit
Arbitrated Loop Physical Address (AL_PA)	A unique one-byte value assigned during loop initialization to each NL_Port on a loop
ASIC	Application Specific Integrated Circuit
Auto Save	Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch
BootP	A type of network server
Buffer credit	A measure of port buffer capacity equal to one frame
Cascade topology	A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.
CHAP	Challenge Handshake Authentication Protocol
Class 2 service	A service which multiplexes frames at frame boundaries to or from one or more N_Ports with acknowledgment provided
Class 3 service	A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment
Default Visibility	Zoning parameter that determines the level of communication among ports/devices when there is no active zone set. It is recommended that all switches have the same Default Visibility setting.
Device security	A component of fabric security that provides for the authorization and authentication of devices that attach to a switch through the use of groups and security sets
Discard Inactive	A zoning configuration parameter that automatically removes the previously active zone set when a zone set is activated on a switch (non-configurable, always enabled)
Configured zone sets	The zone sets stored on a switch excluding the active zone set
DefaultZone	Enables (True) or disables (False) communication among ports/devices that are not defined in the active zone set or when there is no active zone set. This parameter must have the same value throughout the fabric. If interop mode is McDATA Fabric Mode, the Default Zone parameter is automatically distributed throughout the fabric. If McDATA 4Gb SAN Switches are in a fabric with other M-Series directors and edge switches, and the interop mode is Standard/Open Fabric, the Default Zone parameter MUST be disabled (False) on the McDATA 4Gb SAN Switches for zoning to function properly.

Domain ID	User defined number that identifies the switch in the fabric
EFCM	Enterprise Fabric Connectivity Manager
Event log	Log of messages describing events that occur in the fabric
Expansion port	E_Port that connects to another FC-SW-2 compliant switch
Fabric database	The set of fabrics that have been opened during a McDATA Web Server session
Fabric management switch	The switch through which the fabric is managed (the switch connected to the Ethernet network)
Fabric name	User defined name associated with the file that contains user list data for the fabric
Fabric port	An F_Port
Fabric view file	A file containing a set of fabrics that were opened and saved during a previous McDATA Web Server session
Fan Fail LED	An LED that indicates that a cooling fan in the switch is operating below standard
Flash memory	Memory on the switch that contains the chassis control firmware
Force PROM mode	See Maintenance Mode
Frame	Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter
FRU	Field Replaceable Unit
HAFM	High Availability Fabric Manager
Heartbeat LED	A chassis LED that indicates the status of the internal switch processor and the results of the Power On Self Test
Inactive firmware	The firmware image on the switch that is not in use
In-band management	The ability to manage a switch through an FC port
Initiator	The device that initiates a data exchange with a target device
In-order-delivery	A feature that requires that frames be received in the same order in which they were sent
Power LED	A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages
Inter-Switch Link (ISL)	The connection between two switches using E_Ports
Interop mode	Permits interoperation with FC-SW-2 compliant (Standard/McDATA Open mode) switches and switches running in McDATA Fabric Mode (Interop_2 in CLI)
IP	Internet Protocol
LIP	Loop Initialization Primitive sequence
Logged-in LED	A port LED that indicates device login or loop initialization status
Maintenance button	Formerly known as the Force PROM button. Momentary button on the switch used to reset the switch or place the switch in maintenance mode.
Maintenance mode	Formerly known as force PROM mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.
Management Information Base (MIB)	A set of guidelines and definitions for SNMP functions
Management workstation	PC workstation that manages the fabric through the fabric management switch
Mesh topology	A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric
MIB	Management Information Base
Multistage topology	A fabric in which two or more edge switches connect to one or more core switches

NL_Port	Node Loop Port. An FC device port that supports arbitrated loop protocol.
N_Port	Node Port. An FC device port in a point-to-point or fabric connection.
Pending firmware	The firmware image that will be activated upon the next switch reset
PFE key	Product Feature Enablement key. A password that you can purchase from your switch distributor or authorized reseller to enable particular features in your switch
POST	Power On Self Test
Power On Self Test (POST)	Diagnostics that the switch chassis performs at start up
Principal switch	The switch in the fabric that manages domain ID assignments
Product Feature Enablement key	A password that you can purchase from your switch distributor or authorized reseller to enable particular features in your switch
McDATA Web Server	Switch management application
SFP	Small Form-Factor Pluggable
Small Form-Factor Pluggable (SFP)	A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the FC port
SNMP	Simple Network Management Protocol
Target	A storage device that responds to an initiator device
User account	An object stored on a switch that consists of an account name, password, authority level, and expiration date
VCCI	Voluntary Control Council for Interference
World Wide Name (WWN)	A unique 64-bit address assigned to a device by the device manufacturer
WWN	World Wide Name
Zone	Zoning divides the fabric for purposes of controlling discovery. Members of the same zone automatically discover and communicate freely with all other members of the same zone.
Zone set	A set of zones grouped together. The active zone set defines the zoning for a fabric.
Zoning database	The set of zone sets, zones, and aliases stored on a switch

Index

A

- account name
 - display 203, 205
 - factory 105
- active zone set 47, 51
- Active Zoneset data window 47
- Admin
 - account name 108
 - authority 108
- Admin command 110
- Admin session timeout 174
- administrative state
 - configured 77, 100
 - current 77, 100
 - port 100, 169
 - switch 77, 155
- alarm
 - configuration 73, 160
 - configuration defaults 146
 - configuration display 188
 - description 168
 - log 154, 178
- alias
 - add members 60, 111
 - copy 111
 - create 60, 111
 - delete 111
 - delete members 111
 - description 50
 - display list 111
 - display members 111
 - remove 60
 - rename 112
- Alias command 111
- Arbitrated Loop Physical Address 169
- archive configuration 85
- audience 9
- authentication 128
 - device 25
 - trap 84
 - user 25
- authority 108
- authorized reseller, HP 11
- auto save
 - zoning configuration 54

B

- beacon 154
- binding 130
- BootP boot method 82
- broadcast 79, 178
- browser 13
- browser location 15

C

- certificate 30, 121
- CHAP authentication 128
- chassis
 - status 178
- chassis status 178
- checklist 30
- CIM command 113
- CIMListener command 114
- CIMSubscription command 116
- Command Line Interface 105
- command syntax 108
- commands 108
- Common Information Model
 - configure 113
 - display listener 179
 - listener 114
 - service 81, 172
 - subscription 116
- Config command 118
- configuration
 - activate 118
 - archive 85
 - backup 118
 - copy 118
 - delete 118
 - edit 118
 - list 118
 - reset 144
 - restore 86, 119
 - save 119
 - wizard 76
- configured administrative state 77
- connection
 - Secure Socket Layer 121
 - security 30, 171, 172
- contact 84
- conventions
 - document 10
 - text symbols 10
- CRC error 73
- Create command 121
- current administrative state 77

D

- data window
 - Active Security 37
 - Active Zoneset 47
 - Configured Zonesets 72
 - description 20, 22, 24
 - Devices 46, 68
 - Port Information 98
 - Port Statistics 96

- Switch 68
- database
 - fabric 39
 - zoning 52
- date 74
- Date command 124
- Decode error 73
- default
 - configuration 87
 - visibility 57
 - zoning 55
- defaults
 - alarm configuration 146
 - port configuration 145
 - RADIUS configuration 147
 - security configuration 148
 - services configuration 148
 - Simple Network Management Protocol configuration 147
 - switch configuration 145
 - system configuration 148
 - zoning configuration 147
- device
 - authentication 25
 - nickname 49
 - scan 101
 - security 31
- Devices data window 46, 68
- disk space 13
- document
 - conventions 10
 - prerequisites 9
 - related documentation 9
- documentation, HP web site 9
- domain ID
 - binding 130
 - description 77
 - display 179
 - lock 77
- Dynamic Host Configuration Protocol 82

E

- E_Port isolation 61, 77
- embedded GUI service 81
- Error Detect Timeout 80
- event browser
 - filter 45
 - preference 15
 - sort 45
- event logging
 - by component 166, 191
 - by port 167, 192
 - by severity level 192
 - display 191
 - restore defaults 167
 - save settings 167
 - settings 192
 - severity level 44, 167
 - start 167

- stop 167
- event severity 44
- external test 102, 200

F

- F_Port 94, 101
- fabric
 - add 39
 - add a switch 41
 - database 39
 - delete 40
 - displaying information 42
 - loop port 94, 101
 - management 25
 - management workstation 13
 - merge 61
 - port 94, 101
 - rediscovery 40
 - security 30
 - services 37
 - status 42
 - tracker 38
 - tree 20
 - zoning 50
- Fabric Device Management Interface 78, 179
- fabric view file
 - open 40
- faceplate display
 - data window 24
 - description 17, 23
- factory defaults 87, 144
- FC-4 descriptor 101
- FDMI - See Fabric Device Management Interface
- Feature command 125
- File Transfer Protocol
 - example 137
 - service 81, 172
- firmware
 - image file 136
 - install with CLI 90, 126
 - install with McDATA Web Server 90
 - list image files 136
 - non-disruptive activation 89, 135
 - remove image files 136
 - retrieve image file 136
 - unpack image 136
 - version 183
- Firmware Install command 126
- FL_Port 94, 101

G

- gateway address 83, 174
- generic port 94, 101
- graphic window 20
- group
 - add member 35, 127
 - copy 129
 - create 33, 129
 - display 36

- display member 36
- edit member attributes 35, 129
- list 130
- list members 130
- Management Server 129
- remove 35
- remove member 35, 130
- rename 35, 130
- type 129, 130
- Group command 127
- GUI management service 81

H

- hard reset 75
- Hardreset command 132
- hardware status 91
- Heartbeat LED 91
- help 16
- Help command 133
- help, obtaining 11, 12
- History command 134
- host bus adapter 179
- hot reset 75
- Hotreset command 135
- HP
 - authorized reseller 11
 - storage web site 12
 - Subscriber's choice web site 11
 - technical support 11

I

- Image command 136
- in-band management
 - description 79
 - enable 38
- indication service listener 114
- Initial Start Dialog 15
- internal port test 200
- internal test 102
- internet browser 13
- interoperability 80
- IP
 - address 82
 - configuration 82
- IP address 174
- ISL group 129
- ISL monitoring 73

L

- layout 22
- link
 - delete 40
 - selecting 22
 - status 21
- Link control frame preference routing 157
- Link data window 47
- link state database 179
- Lip command 139

- listener
 - add 114
 - Common Information Model 179
 - create 114
 - delete 114
- log
 - archive 166
 - clear 166
 - display 167, 192
 - event 166, 191
 - local 174
 - Power On Self Test 181
 - remote 174
- logged in users 183
- login limit 40, 105
- loop port
 - bypass 169
 - enable 169
 - fabric 94, 101
 - initialization 139
- loopback test 102
- loss of signal monitoring 73

M

- Management Server
 - group 129
 - service 81, 172
- manufacturer information 196
- mask address 174
- McDATA Embedded Web Server 172, 174
- McDATA Web Server
 - start 14
 - user interface 17
- MD5 authentication 128
- media status 95
- memory
 - workstation 13
- memory activity 179
- menu structure 17
- Multi-Frame Sequence bundling 157

N

- name server
 - export 48
- name server display 179
- NDCLA - See Non-Disruptive Code Load and Activation
- network
 - configuration reset 145
 - discovery 82, 174
 - gateway address 174
 - interfaces 179
 - IP address 174
 - mask 174
 - properties 82, 83
- Network Time Protocol
 - client 174
 - description 74
 - interaction with Date command 124
 - server address 174

- service [81](#), [172](#)
- nickname
 - create [49](#)
 - delete [49](#)
 - edit [49](#)
 - export [49](#)
 - import [49](#)
- node-to-node test [103](#)
- non-disruptive activation [89](#), [135](#)
- Non-Disruptive Code Load and Activation [75](#)
- NTP - See Network Time Protocol

O

- online
 - help [16](#)
 - test [103](#)
- operating systems [13](#)
- orphan zone set [51](#)

P

- page break [154](#)
- Passwd command [140](#)
- password
 - change [140](#)
 - factory [105](#)
 - switch [140](#)
 - user account [66](#)
- performance tuning [157](#)
- PFE key [88](#), [125](#)
- Ping command [141](#)
- port
 - administrative state [100](#), [169](#)
 - configuration [100](#), [156](#), [157](#)
 - configuration defaults [145](#)
 - configuration display [188](#)
 - counters [169](#)
 - displaying information [93](#)
 - external test [200](#)
 - group [129](#)
 - initialize [144](#)
 - loopback test [200](#)
 - mode [94](#)
 - online test [200](#)
 - operational information [179](#)
 - operational state [94](#)
 - performance [179](#), [194](#)
 - performance tuning [157](#)
 - reset [102](#)
 - selecting [23](#)
 - speed [95](#), [101](#), [169](#)
 - status [23](#)
 - symbolic name [102](#)
 - test [102](#)
 - type [101](#)
 - view [15](#), [23](#)
- Port Information data window [71](#), [98](#)
- Port Statistics data window [71](#), [96](#)
- port/device tree [53](#)
- Power LED [91](#)

- Power On Self Test log [181](#)
- prerequisites [9](#)
- principal switch [77](#)
- processor [13](#)
- Product Feature Enablement key [88](#)
- properties
 - network [82](#), [83](#)
 - port [100](#)
- Ps command [142](#)

Q

- Quit command [143](#)

R

- RADIUS - See Remote Authentication Dial-In User Service
- RADIUS server
 - add [26](#)
 - authentication order [29](#)
 - configuration [170](#)
 - configuration defaults [147](#)
 - configuration display [196](#)
 - edit configuration [28](#)
 - remove [27](#)
 - reset [144](#)
- read community [84](#)
- refresh [42](#), [68](#)
- related documentation [9](#)
- Remote Authentication Dial-In User Service
 - server [25](#)
- remote log
 - configuration [83](#)
 - enable [174](#)
 - host address [174](#)
- reset
 - with POST [75](#)
 - without POST [75](#)
- Reset command [144](#)
- Resource Allocation Timeout [80](#)
- restore configuration [86](#)
- Reverse Address Resolution Protocol [82](#)

S

- scan device [101](#)
- secret [128](#)
- Secure Shell
 - description [30](#)
 - service [81](#)
- Secure Shell service [171](#)
- Secure Socket Layer
 - certificate [121](#)
 - description [30](#)
 - service [81](#), [172](#)
 - switch time [124](#)
- security
 - certificate [30](#)
 - configuration [36](#), [158](#)
 - configuration defaults [148](#)
 - configuration display [188](#)

- connection 30
- consistency checklist 30
- database 144
- device 31
- fabric 30
- user account 30
- Security command 149
- security database
 - clear 35, 149
 - display 149
 - display history 149
 - limits 149
- security edit session
 - cancel 149
 - initiate 149
 - revert changes 149
 - save changes 150
- security set
 - activate 37, 152
 - add member group 152
 - copy 152
 - create 33, 152
 - deactivate 37, 152
 - delete 152
 - delete member group 153
 - display 36, 153
 - display active 149, 152
 - display members 152
 - remove 35
 - rename 35, 153
- Securityset command 152
- SerDes level test 102
- service listener 114
- services 80
- services configuration defaults 148
- Set command 154
- Set Config command 156
- Set Log command 166
- Set Port command 169
- Set Setup command 170
- severity levels 44
- SFP level test 102
- SHA-1 authentication 128
- Show command 178
- Show Config command 188
- Show Log command 191
- Show Perf command 194
- Show Setup command 196
- Shutdown command 199
- Simple Network Management Protocol
 - configuration 84, 173
 - configuration display 196
 - defaults 147
 - enable 38, 84
 - proxy 84
 - reset 144
 - service 81, 172
 - trap configuration 85
- static boot method 82

- status icon color 20
- steering 181
- subnet mask address 83
- Subscriber's choice, HP 11
- subscription
 - create 116
 - delete 116
- support file 88, 121
- switch
 - add 41
 - administrative state 77, 155
 - advanced properties 79
 - configuration 76, 159
 - configuration defaults 145
 - configuration display 188
 - delete 40
 - displaying information 68
 - hard reset 75, 132
 - hot reset 75
 - icons 43
 - location 84
 - log 174
 - management service 81, 171
 - manufacturer information 196
 - operational information 182
 - paging 74
 - properties 76
 - replace 41
 - reset 75, 202
 - reset without POST 75, 144
 - restore factory defaults 87
 - selecting 22
 - services 144, 171, 196
 - status 21
- Switch data window 68
- symbolic name
 - port 102
 - switch 76
- symbols in text 10
- syslog 83
- system configuration
 - change 174
 - defaults 148
 - display 196
- System Fault LED 91
- system services 80

T

- technical support, HP 11
- Telnet
 - service 81, 171
 - session timeout 174
- Test command 200
- testing ports 102
- text symbols 10
- time 74, 124
- time zone 155
- timeout
 - Admin session 174

- Telnet session [174](#)
- values [80](#)
- tool bar
 - standard [19](#)
 - zoning [53](#)
- topology display
 - arrange icons [22](#)
 - data windows [22](#)
 - description [17](#)
 - usage [21](#)
- transceiver status [95](#)
- transmission speed [101](#)
- trap
 - authentication [84](#)
 - community [84](#)
 - configuration [85](#)
 - SNMP version [85](#)

U

- upgrade [125](#)
- Uptime command [202](#)
- user account
 - add [203](#)
 - admin [105](#)
 - admin account [105](#)
 - create [64](#)
 - default [63](#)
 - delete [203](#)
 - display [203](#)
 - edit [203](#)
 - list [203](#)
 - logged in [183](#)
 - modify [67](#)
 - password [66](#)
 - remove [65](#)
 - security [30](#)
- User command [203](#)

V

- version snapshot
 - compare [39](#)
 - export [39](#)
 - save [39](#)
- Virtual Interface preference routing [157](#)

W

- web server [172](#), [174](#)
 - service [81](#)
- web sites
 - HP documentation [9](#)
 - HP storage [12](#)
 - HP Subscriber's choice [11](#)
- Whoami command [205](#)
- wizard
 - configuration [76](#)
- working
 - directory [15](#)
 - status indicator [21](#)

- workstation requirements [13](#)
- write community [84](#)

Z

- zone
 - add member port [58](#), [206](#)
 - copy [57](#), [206](#)
 - create [206](#)
 - definition [50](#)
 - delete [206](#)
 - delete member port [207](#)
 - list [206](#)
 - list members [206](#)
 - remove all [59](#)
 - remove member port [59](#)
 - rename [59](#), [207](#)
 - type [207](#)
- Zone command [206](#)
- zone merge
 - description [61](#)
 - failure [61](#)
 - failure recovery [61](#)
- zone set
 - activate [57](#), [209](#)
 - active [47](#), [51](#), [211](#)
 - add member zone [209](#)
 - copy [209](#)
 - create [56](#), [209](#)
 - deactivate [57](#), [145](#), [209](#)
 - definition [51](#)
 - delete [209](#)
 - delete member zone [209](#)
 - display [209](#)
 - display active [209](#)
 - display members [210](#)
 - display zones [207](#)
 - management [56](#)
 - orphan [51](#)
 - remove [57](#)
 - rename [59](#), [209](#)
 - tree [53](#)
- Zoneset command [209](#)
- zoning [80](#)
 - configuration [54](#), [161](#)
 - configuration defaults [147](#)
 - configuration display [188](#)
 - database [51](#), [52](#), [145](#)
 - default [55](#)
 - edit [211](#)
 - history [211](#)
 - limits [212](#)
 - list definitions [212](#)
 - remove all [56](#)
 - revert changes [212](#)
 - save edits [212](#)
- Zoning command [211](#)
- zoning database
 - save to file [55](#)